09/658,565

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 １月２５日

出 願 番 号
Application Number: 特願２０００－０１６２８５

出 願 人
Applicant (s): 株式会社東芝

２０００年 ６月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３０４４３０１

【書類名】　特許願

【整理番号】　A000000159

【提出日】　平成12年 1月25日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　5/00

【発明の名称】　埋め込み符号生成装置及び埋め込み符号検出装置とこれらを用いた電子透かし埋め込み装置及び電子透かし検出装置

【請求項の数】　20

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　村谷　博文

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【先の出願に基づく優先権主張】

【出願番号】　平成11年特許願第280652号

【出願日】　平成11年 9月30日

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　埋め込み符号生成装置及び埋め込み符号検出装置とこれらを用いた電子透かし埋め込み装置及び電子透かし検出装置

【特許請求の範囲】

【請求項１】

入力された利用者識別番号に対して、互いに素な複数の整数を法とする複数の剰余を求める剰余計算手段と、

前記剰余計算手段により求められた各剰余を表す符号であって、所定のビット数を一単位とする連続した１の列及び０の列で構成される複数の部分符号を生成する部分符号生成手段と、

前記部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成する連接手段とを具備することを特徴とする埋め込み符号生成装置。

【請求項２】

所定のビット数を一単位とする連続した１の列及び０の列で構成される複数の部分符号を連接した埋め込み符号を各部分符号に分割する符号分割手段と、

分割された各部分符号をそれぞれ復号して予め定められた互いに素な複数の整数を法とする２つの剰余からなる複数の剰余対を得る部分符号復号手段と、

前記複数の剰余対から結託者の利用者識別番号を計算する結託者番号計算手段とを具備することを特徴とする埋め込み符号検出装置。

【請求項３】

前記複数の剰余対から結託の有無を判定する結託判定手段をさらに有し、前記結託者番号計算手段は該結託判定手段により結託があると判定されたとき前記結託者の利用者識別番号を計算することを特徴とする請求項４記載の埋め込み符号検出装置。

【請求項４】

前記結託者番号計算手段は、入力されたｋ′個の剰余対の各々から一方の剰余を選択してｋ′個の剰余の組（ｒ１，ｒ２，…，ｒｋ′）を生成する剰余選択部と、

前記剰余選択部により生成されたｋ′個の剰余の組からｋ個の剰余（ｒ１，ｒ

２，…，ｒｋ）を選択する一貫性選択部と、

前記一貫性選択部により選択されたｋ個の剰余から中国剰余定理に従って結託者の利用者識別番号ｕの候補を計算する中国剰余定理部とからなり、

前記一貫性検査部は、前記中国剰余定理部により計算された結託者の利用者識別番号ｕの候補と残りの（ｋ′－ｋ）個の剰余のうちの所定個数（ｙ）の剰余との間にｒｉ＝ｕ ｍｏｄ ｐｉ（ｉ＝１，…，ｙ）が成立するか否かを判定し、この関係が成立する場合、ｕを結託の利用者識別番号として出力し、この関係が成立しない場合には前記剰余選択部に対して新たなｋ′個の剰余の組を要求し、結託者の利用者識別番号が特定できるまで新たな候補について同様の処理を繰り返すことを特徴とする請求項１または２記載の埋め込み符号検出装置。

【請求項５】

入力された利用者識別番号に対応して複数の整数要素の組を計算する計算手段と、

所定個数の利用者識別番号に対して前記計算手段により計算される全ての整数要素の組を表現可能なｋ′個の部分符号のうちのｋ個の組み合わせが前記利用者識別番号を一意に表現できる部分符号を前記各整数要素に対応してそれぞれ生成する部分符号生成手段と、

前記部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成する連接手段とを具備し、

前記ｋ′は、３以上の正整数をｃ、１以上の正整数を、前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数をｑとして、ｃ（ｋ＋１）／ｑ以上となるように決定されていることを特徴とする埋込み符号生成装置。

【請求項６】

前記所定個数の利用者識別番号に対して前記計算手段により計算される各整数要素のとりうる値の個数をp_i（ｉ＝１，２，…，ｋ′）とし、前記埋め込み符号の検出時に想定される検出誤り率をεとしたとき、前記ｋ′は、

【数１】

$$\left[1-\prod_{i=1}^{l}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+l)/2C_{k+l}\times 2^{k+l}} \geq 1-\frac{\varepsilon}{2} \qquad (1)$$

の条件を満たすように設定されていることを特徴とする請求項５記載の埋め込み符号生成装置。

【請求項７】

前記計算手段は、前記入力された利用者識別番号に対応して互いに素な複数の整数を法とする剰余の組を前記整数要素の組として計算することを特徴とする請求項５または６記載の埋め込み符号生成装置。

【請求項８】

前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算することを特徴とする請求項５記載の埋め込み符号生成装置。

【請求項９】

前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算するものであり、

前記p_i（ｉ＝１，２，…，ｋ′）を同一の正整数ｐとして、

【数２】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p - 1} \qquad (2)$$

の条件をさらに満たすことを特徴とする請求項６記載の埋め込み符号生成装置。

【請求項１０】

所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なｋ′個の部分符号のうちのｋ個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要

素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、

抽出された各部分符号に分割する符号分割手段と、

分割された各部分符号をそれぞれ復号する部分符号復号手段と、

各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、

前記ｋ′は、３以上の正整数をｃ、１以上の正整数を、前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数をｑとして、ｃ（ｋ＋１）／ｑ以上となるように決定されていることを特徴とする埋込み符号検出装置。

【請求項１１】

前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値をp_i（ｉ＝１，２，…，ｋ′）とし、前記埋め込み符号の検出時に想定される検出誤り率をεとしたとき、前記ｋ′は、

【数３】

$$\left[1-\prod_{i=1}^{l}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{(k+1)/2\,C_{k+1}\times 2^{k+1}} \geq 1-\frac{\varepsilon}{2} \qquad (1)$$

の条件を満たすように設定されていることを特徴とする請求項１０記載の埋め込み符号検出装置。

【請求項１２】

前記整数要素の組は、前記利用者識別番号に対応して計算された互いに素な複数の整数を法とする剰余の組であることを特徴とする請求項１０または１１記載の埋め込み符号検出装置。

【請求項１３】

前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であることを特徴とする請求項１

０記載の埋め込み符号検出装置。

【請求項１４】

前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、

前記p_i（ｉ＝１，２，…，ｋ′）を同一の正整数ｐとして、

【数４】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p-1} \qquad (2)$$

の条件をさらに満たすことを特徴とする請求項１１記載の埋め込み符号検出装置。

【請求項１５】

所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なｋ′個の部分符号のうちのｋ個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、

抽出された各部分符号に分割する符号分割手段と、

分割された各部分符号をそれぞれ復号する部分符号復号手段と、

各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、

前記部分符号復号手段は、前記各部分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“１”のビット数を計数する計数部と、該計数部で得られた計数値が第１の閾値を越えているか否かを判定する第１の判定部と、前記計数値が第２の閾値に満たないか否かを判定する第２の判定部と、前記第１の判定部で第１の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第２の判定部で第２の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大値決定部の決定結果を復号結果として出力することを特徴とする埋め込み符号検出

装置。

【請求項１６】

請求項１、５乃至９のいずれか１項に記載の埋め込み符号生成装置によって生成された埋め込み符号を埋め込み対象コンテンツに透かし情報として埋め込む電子透かし埋め込み装置。

【請求項１７】

埋め込み対象コンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語を前記透かし情報として前記埋め込み対象コンテンツに埋め込む手段と

を具備することを特徴とする電子透かし埋め込み装置。

【請求項１８】

入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語と前記コンテンツとの相関値を求める手段と、

前記相関値に基づいて前記コンテンツ中の前記入力された利用者識別番号に対応する符号語の有無を判定する手段と

を具備することを特徴とする電子透かし検出装置。

【請求項１９】

入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、

予め登録された複数の利用者識別番号にそれぞれ対応する、シンプレックス符号を構成する複数の符号語を出力する手段と、

出力された各符号語と前記コンテンツとの各相関値を求める手段と、

求められた各相関値をベクトルとみなして計算されたノルムに基づいて前記コ

ンテンツ中の透かし情報の有無を判定し、透かし情報があると判定した場合に前記相関値に基づいて結託者を特定する手段と
を具備することを特徴とする電子透かし検出装置。

【請求項２０】

請求項１または５乃至９のいずれか１項に記載の埋め込み符号生成装置によって生成された埋め込み符号が透かし情報として埋め込まれたコンテンツを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタルデータ化された音声、音楽、動画、静止画等のコンテンツに対して透かし情報を埋め込む電子透かし埋め込み装置及び埋め込み済コンテンツから透かし情報を検出する電子透かし検出装置に関する。

【０００２】

【従来の技術】

電子透かし(digital watermarking)は、ディジタルデータ化された音声、音楽、動画、静止画等のコンテンツに対して、これらのコンテンツの著作権者や利用者の識別情報、著作権者の権利情報、そのデータの利用条件、その利用時に必要な秘密情報、コピー制御情報などの情報(これらを透かし情報と呼ぶ)を知覚が容易ではない状態となるように埋め込み、後に必要に応じて透かし情報をそのデータ内から検出することによって利用制御、コピー制御を含む著作権保護を行ったり、二次利用の促進を行うための技術である。

【０００３】

[電子透かしの要件]

不正利用の防止を目的とする場合、電子透かし技術はディジタル著作物に対して通常に施されると想定される各種の操作や意図的な攻撃によって、透かし情報が消失したり改竄されたりしないような性質(ロバスト性)を持つ必要がある。例えば、静止画や動画はそれぞれＪＰＥＧ(Joint Photographic Coding Experts Group)符号化、ＭＰＥＧ(Moving Picture Experts Group)符号化と呼ばれる非可

逆圧縮を施されることが多いため、電子透かし技術はこれらの非可逆圧縮に対するロバスト性を持つことが重要な要件となることが通常である。

【０００４】

[電子透かしの分類]

従来、画像に対する電子透かしの方式は、画素領域利用型と周波数領域利用型に大別することができる。画素領域利用型の電子透かし方式は、画素値を変更することで直接的に透かし情報の埋め込みを行うものである。一方、周波数領域利用型の電子透かし方式は、直交変換によって、一旦、画素領域から周波数領域へ移り、周波数領域において埋め込みを行った後、再び、逆直交変換によって周波数領域から画素領域に戻るものである。透かし情報は波として埋め込まれることになる。

【０００５】

[周波数領域利用型電子透かし方式]

周波数領域利用型の電子透かし方式としては、例えば文献[１] Koch, E. and Zhao, J., “Towards Robust and Hidden Image Copyright Labeling”, Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, 452-455, June 20-22, 1995.(Koch-Zhaoの方式という)や、文献[２]Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T., “Secure Spread Spectrum Watermarking for Multimedia”, NEC Research Institute, Technical Report 95-10, 1995.(Coxらの方式という)がある。これらの方式では、埋め込み対象となる周波数成分を非可逆圧縮による影響が小さな低周波数から中間周波数に設定することで非可逆圧縮に対するロバスト性を実現している。

【０００６】

[画素領域利用型電子透かし方式]

画素領域利用型の電子透かし方式としては、画素値のＬＳＢを変更することで埋め込みを行う方式がある。その変更は、擬似乱数系列(ＰＮ系列)に従って(文献[３] Schyndel, R.G. van, Tirkel, A.Z., and Osborne, C.F., “A Digital Watermark”, Proceedings of 1st IEEE International Conference on Image Processing, 1994.あるいは文献[４] Wolfganf, R.B. and Delp, E.J., “A Wate

rmark for Digital Images”，ICIP96，219-222，1996.)、あるいは予め用意したマスクパターンに従って(文献[５] Pitas，I.，“A Method for Signature casting on Digital Images”，ICIP96，215-218，1996.)、ある固定の大きさの変分を加えるか減ずるかを決定することで行う。この方式は、非可逆圧縮に対するロバスト性はあまり良くない。

【０００７】

[スペクトラム拡散による電子透かし]

スペクトラム拡散(spread spectrum)の考えを適用することで非可逆圧縮へのロバスト性を高める方式がある。スペクトラム拡散とは、通信したい信号に必要な帯域に比べて十分大きな帯域中に、情報を広く分散させて伝送する通信方式をいう(文献[６] 山内雪路，“スペクトラム拡散通信”，東京電機大学出版局，1994.)。伝送路上のノイズに対する耐性が優れている。元のコンテンツを搬送波、透かし情報を希望波、非可逆圧縮による影響を干渉波(ノイズ)とみなすことで、スペクトラム拡散の考えを電子透かし技術へ適用する。

【０００８】

スペクトラム拡散による電子透かし方式として、画素領域における拡散(文献[７] Smith，J.R. and Comiskey，B.O.，“Modulation and Information Hiding in Images”，Information Hiding，207-226，1996.、文献[８]大西淳児,岡一博,松井甲子雄，“PN系列による画像への透かし署名”，SCIS97，26B，1997.)と、周波数領域における拡散(先の文献[２]参照)が提案されている。文献[２]の方式と文献[８]の方式は、それぞれ摂動法、直接拡散法(direct sequence spread spectrum)と呼ばれることがある(文献[９] 松井甲子雄，“電子透かしの基礎－マルチメディアのニュープロテクト技術－”，森北出版株式会社,1998.)。

【０００９】

[周波数領域における拡散(摂動法)]

先の文献[１]の方式では、透かし情報の埋め込みは画素値に対して直交変換を行い、周波数領域において透かし情報を拡散して埋め込む。拡散は、周波数領域において複数の周波数成分の値とある乱数列に従って変化させることによって行う。拡散後、逆直交変換を行う。透かし情報の検出は、画素値に対して直交変換

を行い、埋め込みが行われた周波数成分の値を埋め込みに用いられた乱数列の間の相関値によって判定を行う。埋め込まれた透かし情報は、画素領域では、画像(ブロック)全体に分散されているため、各種の操作に対してロバストである。また、透かし情報を埋め込んだ周波数成分が低中間周波数領域にあるならば、低周波数通過フィルタによっても透かし情報が失われにくい。

【００１０】

[画素領域における拡散(直接拡散法)]

一方、文献[８]の方式では、透かし情報の埋め込みは、ＰＮ(pseudo-random noise)系列を画素値に乗積することにより直接拡散する。得られた画像に対して直交変換を行い、周波数領域において透かし情報を埋め込み、再び逆直交変換を行う。その後、同じＰＮ系列を画素値に乗積して、逆拡散を行う。透かし情報の検出は、ＰＮ系列によって画素値を直接拡散する。得られた画像に対して直交変換を行い、透かし情報の埋め込みを行った周波数成分の値から判定する。直接拡散法では、画素値をＰＮ系列で変調するため、透かし情報は高周波成分に偏り、摂動法と比較して、ＪＰＥＧ圧縮等やＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ変換に対して、透かし情報が失われやすい。

【００１１】

[スペクトラム拡散の処理コストの軽減]

本発明者らは、ＪＰＥＧ圧縮等の下で透かし情報が失われにくくするために、透かし情報を埋め込むブロックサイズを大きくする方式を提案した(文献[１０]村谷博文,加藤拓,遠藤直樹，“直接拡散による電子透かしの耐性評価”，SCIS99，II，503-508，1999.)。

【００１２】

従来より、大きなブロックサイズの画像に対する埋め込みは行われていたが、この方式では大きなブロックに対する直交変換の処理コストを軽減することで埋込みおよび検出処理の低コストと高速性を実現した。この方式は、画像の周波数成分に依存しないか、あるいは、少数の周波数成分値にしか依存しない埋込み位置や埋込み強度を採用するため、摂動法よりも直接拡散法に適していた。しかし、この方式は大きなブロックサイズを選択したため、大きなサイズの透かし情報

を埋め込むことが難しかった。

【００１３】

この問題に対しては、ブロック毎の画像の局所性に応じた埋め込みを行う「画像適応(image adaptation)」によって、小さな埋込み強度で埋め込みを行うことを可能にし、透かし情報のサイズを増加させる方法がある。この方法は例えば、文献[１１]Boland, F.M., O Ruanaidh, J.J.K., and Dautzenberg, C., “Water marking Digital Images for Copyright Protection”, Proceedings of the fifth International Conference on Image Processing and its Application, 1995.(Boland等という)や、先の文献[８]に記載された方式で採用されている。

【００１４】

ところが、これら文献[１１]や先の文献[８]の方式では、埋め込み強度は多数の周波数成分の値から決定されるため、本質的に直交変換を避けることができなくなってしまう。従って、直交変換を行うことなく、画素値から直接に埋め込み強度を決定する方式をとることが望ましい。

【００１５】

[フィンガープリンティング]

大きなサイズの透かし情報をＪＰＥＧ圧縮等に対してロバストに埋め込むことができる電子透かし方式において、そのコンテンツ提供先の利用者を特定する情報を埋め込む応用形態が考えられる。このような応用形態は「フィンガープリンティング」と呼ばれる。海賊版の再配布を抑止する効果が期待できる。

【００１６】

[結託攻撃問題]

ところが、同じコンテンツに異なる透かし情報が埋め込まれた複数の埋め込み済みコンテンツが存在する場合、それら複数の埋め込み済コンテンツを利用して透かし情報を改竄、消失させるという行為が考えられる。このような行為は、「結託攻撃(collusion attack)」と呼ばれている。結託攻撃では、複数の埋め込み済みコンテンツの画素値を平均化することで新たなコンテンツを偽造したり、値が異なる画素値や周波数成分値の部分に対して、ランダムに、あるいは、多数決／少数決に従って値を変更する、などのやり方で改変を加える。

【００１７】

[結託攻撃に対する従来の対策]

従来、結託攻撃に対処する方法として、スペクトラム拡散による方法(先の文献[2]、及び文献[１２]山本哲也，渡辺創，嵩忠雄，“すべての結託ユーザを特定可能な電子透かし法”，SCIS'98，10.2.B，1998.)と、符号理論的な方法(文献[１３] Boneh, Dan and Shaw, James, “Collusion-Secure Fingerprinting for Digital Data”，CRYPTO'95，452-465，1995.、文献[１４]鈴置昌宏，渡辺創，嵩忠雄，“結託攻撃に強い電子透かし法”，SCIS'97，31B，1997.及び文献[１５] 吉田淳，岩村恵市，今井秀樹，“画質劣化が少なく結託攻撃に強い電子透かし法”，SCIS'98，10.2.A，1998.)が提案されている。

【００１８】

文献[2]の方法によれば、利用者毎にＮ(０，１)に従う相異なる実乱数列が与えられる。２つの異なる実乱数列の間に相関がないとする。結託攻撃は、画素値を平均化する操作とする。結託によって、検出時の相関値は減衰してしまう。

【００１９】

文献[2]では、相関値の代わりに、定義された類似度によって結託の検出を行う。この類似度は、相関値を検出された透かし情報のノルムで除したものとして定義される。結託により電子透かしのノルムも減衰しているので、相関値が減衰しても類似度はさほど減衰しない。これにより結託者全員を特定することができる。ただし、この方法は検出において埋め込み対象であった原画像を必要とし、また結託者特定に時間がかかるのが難点である。

【００２０】

文献[１２]では、むしろ平均化による結託攻撃の際の相関値の減衰という性質を利用した結託者の特定方法を提案している。結託者間で共通の電子透かしは減衰せず、それ以外の電子透かしは減衰するので、埋め込み時のレベルを保っている電子透かしの組から結託者の組を特定する。全利用者数をｎ、想定する最大の結託者数をｃとすると、$(c+1)(c-1)\log_{c+1} n$オーダの長さの符号で結託者を特定することができる。ただし、この方法はスペクトラム拡散法に特有の性質を利用するため、すべての電子透かし方式に適用が可能なわけではない。

〔００２１〕

先の文献[１３]には、透かし情報を表現する符号において、すべての結託者の間で共通な値を持つビットは検出不能であるという性質を利用して、検出不能なビットがそのまま残るならば、それ以外のビットを如何に変更しようとも、結託者以外の利用者の符号を生成することができない符号(c-frameproof符号と呼ばれる)を構成して透かし情報とする方式が提案されている。

〔００２２〕

この方式では、誰のものでもない符号が生成される可能性は残るものの、これにより、ある利用者が自らのコンテンツをそのまま再配布した場合(native redistribution)、その利用者は他者の結託によるものであると主張しての否認はできなくなる。

〔００２３〕

結託者の総数に制限が無いn-frameproof符号は、符号サイズがｎとなる。結託者総数が最大cであるc-frameproof符号は、符号サイズが$16c^2 \log n$（ｃは結託者数、ｎは全利用者数)である。

〔００２４〕

文献[１３]ではさらに、２組の結託者のグループがあって、共通部分が空集合の場合、それぞれのグループ内での結託によって生成できる符号(feasible set)の集合間の共通部分も空集合であるような符号(totally c-secure符号)は存在しないということを示している。つまり、結託攻撃によって誰のものでもない符号を生成することができない符号は、厳密には存在しないことを示した。

〔００２５〕

そこで、文献[１３]では結託者数がｃ人以内の場合に結託者を誤って指摘する確率がε以下である符号(c-secure code with ε-error)を構成した。まず、誤りεを持つn-secure符号$\Gamma(n, 2n^2 \log(2n/\varepsilon))$を構成した。その符号サイズは、$2n^2(n-1)\log(2n/\varepsilon)$である。

〔００２６〕

さらに、それをTraitor Tracingスキーム(文献[１６]Chor, B., Fiat, A. and Naor, M., “Tracing traitors”, Proceedings of CRYPTO'94, 257-270, 1994

.)と組合せて誤りがε以下のc-secure符号の可能性を示した。この符号の符号サイズは、Ｏ(ｃ^{4} log(ｎ／ε) log(１／ε))である。

【００２７】

[Chernoffの限界(Chernoff bound)]

文献[１６]では、Traitor Tracingスキームにおいて、Chernoffの限界の式を利用して結託者を特定するために必要な利用者固有鍵の数を決定している。先の文献[１３]では、その方法を流用して誤りεのn-secure符号やc-secure符号を構成した。平均値ｐの独立なｎ個の確率変数$X_i \in \{0, 1\}$があるとき、これらの和が平均値からずれる確率の限界を与えるのがChernoffの限界である。上端と下端の限界は、それぞれ次式で与えられる。

【００２８】

【数５】

$$\Pr[\sum_{i=1}^{n} X_i - np > n\delta] < \{\exp(\delta/p)/(1+\delta/p)^{1+\delta/p}\}^{np}$$

$$\Pr[\sum_{i=1}^{n} X_i - np < -n\delta] < \{\exp(-\delta/p)/(1-\delta/p)^{1-\delta/p}\}^{np}$$

【００２９】

さらに、緩い限界として次式が成り立つ。

【００３０】

【数６】

$$\Pr[|\sum_{i=1}^{n} X_i - np| > n\delta] < 2\cdot\exp\{-\delta^2 n/(2p(1-p))\}$$

【００３１】

ここで、０≦δ＜ｐ(１－ｐ)とする。また、次式が成り立つ。

【００３２】

【数７】

$$\Pr[\sum_{i=1}^{n} X_i - np < -n\delta] < \exp\{-\delta^2 n/(2p^2)\}$$

【００３３】

[結託者中の２人のみを指摘する方法]

文献[１３]で提案されている誤りεのn-secure符号やc-secure符号は、できるだけ多数の結託者を指摘するように設計されていた。利用者を順序集合とみなし、文献[４]で示されているΓ_0(ｎ，ｄ)符号を、結託者の集合の中から最大と最小の２人を特定する符号として利用することもできる。この場合には、より小さな符号サイズでの構成が可能である。

【００３４】

ここで、Γ_0(ｎ，ｄ)符号とはｄビットを一単位とする連続した１の列及び０の列で構成される符号であり、このような１の列や０の列を符号数ｎに応じた単位数だけ並べて構成される。従って、この符号では１と０はそれぞれｄビットを単位として連続するように配置され、ｄビット未満の数の１や０が孤立して存在することはない。

【００３５】

例えば、ｄ＝３，ｎ＝５とすれば、Γ_0(ｎ，ｄ)符号であるΓ_0(５，３)符号は以下のようになる。

１１１　１１１　１１１　１１１
０００　１１１　１１１　１１１
０００　０００　０００　１１１
０００　０００　０００　１１１
０００　０００　０００　０００

文献[１４]では、２つの符号を昇順と降順に重ね合わせた符号を利用し、結託者中の２人を特定するn-secure符号を提案している。この符号の符号サイズは、$2n\log_4(2/\varepsilon) = n\log_2(2/\varepsilon)$となる。文献[１５]では、Γ0(ｎ，ｄ)符号において０＜weight(ｘ$|_{Bs}$)となる最小のＳ(Ｓmin)と、weight(ｘ$|_{Bs}$)＜ｄと

なる最大のＳ(Ｓmax)を求め、ＳminとＳmax＋１を結託者であると指摘するアルゴリズムによって結託者の２人を特定する方法を示した。この符号の場合、誤りεのn-secure符号は、符号サイズが$(n-1)\log_2(2/\varepsilon)$となる。

〔００３６〕

[誤りεの2-secure符号]

結託者総数が小さな場合には、符号サイズを小さくすることが可能である。先の文献[１５]には、結託者総数２人の場合に結託者の両方を指摘する符号であって、その符号サイズが$3n^{1/2}-1\ \log_2(6/\varepsilon)$の符号を示している。

〔００３７〕

[結託攻撃耐性の限界]

文献[１７] Ergun, Funde, Joe Kilian and Ravi Kumar, "A Note on the Limits of Collusion-Resistant Watermarking", EUROCRYPT'99, 140-149, 1999.)は、電子透かし方式の詳細に依存せずに、結託攻撃に対する耐性には限界があることを理論的に示した。その主張は、正しい結託者を指摘する確率を高くしようとすると、誤った利用者を結託者として指摘してしまう確率(偽陽性率)が高くなってしまうというものであった。

〔００３８〕

文献[１７]で想定している結託攻撃は、図２６に示すように異なるすかし情報が埋め込まれた複数のコンテンツ(コンテンツ１，コンテンツ２，コンテンツ３)を平均化し、その後、ランダムな擾乱を加えるというものである。Ergun等の観点から、例えば先の文献[１３]での議論を捉えなおしてみる。文献[１３]における議論では、確率論的なc-secure符号の構成要素として$\Gamma_0(n, d)$符号を用いている。この$\Gamma_0(n, d)$符号は、図２７(ｄ＝３の例)のように(1,1,1)と(-1,-1,-1)に符号をとる符号化をｎ重に直積して得られる。

〔００３９〕

この$\Gamma_0(n, d)$符号に対して、文献[１７]で提案された結託攻撃を適用すると、平均化によって得られるコンテンツは、(1,1,1)と(-1,-1,-1)を結ぶ直線上にある重心に移る。結託攻撃は、さらに、その重心からずれた位置にコンテンツを移す。この場合、結託攻撃後のコンテンツが(1,1,1)か(-1,-1,-1)の近傍にあ

る場合には、これは結託攻撃によって変更されていないと判断し、原点付近にある場合には結託攻撃によって変更されたとみなすことになる。

〔００４０〕

このΓ$_0$(ｎ，ｄ)符号において、結託者のうち(1,1,1)の符号を持つ者の数と(-1,-1,-1)の符号を持つ者の数の間に大きな偏りがある場合、平均化の結果、重心は(1,1,1)あるいは(-1,-1,-1)のかなり近くに位置することとなる。その後、ランダムな擾乱を受けるので、一般に、結託者を特定するアルゴリズムは、コンテンツが(1,1,1)または(-1,-1,-1)から擾乱によって移ったものか、重心から擾乱によって移ったものかを誤って判断する可能性が高い。つまり、Ergun等自身、かれらの結論がほとんどの電子透かしアルゴリズムに適用されると言明しているが、Boneh等の符号化もErgun等の限界を逃れることはできないといえる。

〔００４１〕

一方、Γ$_0$(ｎ，ｄ)符号において、２つの符号間の最大距離はｎｄ、最小距離はｄと幅が大きい(図２８参照)。Γ$_0$(ｎ，ｄ)符号は結託攻撃への耐性に重点がおかれいることから、受信空間中に非常にスパースに符号語が配置されているためである。

〔００４２〕

電子透かしアルゴリズムは、コンテンツの品質への影響がないように、符号間の最大距離ｎｄの符号を埋め込む必要がある。電子透かしアルゴリズムが、Γ$_0$(ｎ，ｄ)符号をコンテンツ空間へ埋め込み、その埋め込みが、符号間の距離とコンテンツ間の距離とが比例するような性質を持つ場合、オリジナルのコンテンツとの透かし情報を埋め込んだ後のコンテンツとの間の最大距離もｎｄ／２以上となるので、ｎｄが大きな場合には、コンテンツ品質への影響が大きくなる(図２９の埋め込み１)。

〔００４３〕

仮に、これを避けるため、電子透かしアルゴリズムが符号をコンテンツ空間中のオリジナルコンテンツからの距離関係が保たれないような埋め込みによって、すべての符号語がオリジナルコンテンツとほぼ等しい距離にあるようにしたとすると、Γ$_0$(ｎ，ｄ)符号がもともと持っていた結託攻撃への耐性の根拠が失われ

てしまうことになる(図２９の埋込み２)。

【００４４】

つまり、Ergun等の限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式を実現することが望ましいと考えられる。

【００４５】

(スペクトラム拡散による電子透かしの結託攻撃耐性)

一方、スペクトラム拡散による電子透かし方式では、埋め込みの影響がコンテンツ品質に大きな影響を与えないように埋め込み強度が設定される。その上で、埋め込みに用いる擬似乱数列が符号語に対応する。

【００４６】

標本値空間と周波数空間の間の直交変換は線形写像なので、攻撃対象の電子透かし方式が空間領域利用型であれ周波数領域利用型であれ、Ergun等の結託攻撃は擬似乱数列を平均化して、さらに擾乱を与えるという操作となる。

【００４７】

スペクトラム拡散による電子透かし方式では、符号語である擬似乱数列は相互相関(cross-correlation)がほとんどゼロとなるように選択されることが普通である。従って、ｋ個のコンテンツの平均によって得られるコンテンツは、ある結託者に対応する擬似乱数列との相関が１／ｋに減衰すると考えられる。擬似乱数列間の相互相関が十分小さく、かつ、このｋがあまり大きくなければ、電子透かしの検出において相関値があるあらかじめ定められた閾値を越えるため、結託者を特定することが可能である。

【００４８】

前述した文献[２]の方式は、検出においてオリジナルコンテンツを利用することを前提としており、相関値の代わりに類似度(similarity)と呼ばれる量を用いて検出が行われる。類似度は、検出対象コンテンツからオリジナルコンテンツを引いた差分と埋め込みに用いた擬似乱数列の間の相互相関値を差分の自己相関値の平方根で正規化したものである。

【００４９】

類似度による検出では、結託攻撃における平均化によって、分子の相関値が１／ｋに減衰するが、分母の差分のノルムも１／ｋに減衰するため、類似度は減衰しないことが期待される。ただし、平均化以外にノイズが加わる場合には、そのノイズの影響は正規化によってかえって大きくなる。

【００５０】

文献[１８] Kilian, Joe, F.Thomas Leighton, Lesley R. Matheson, Talal G. Shamoon, Robert E. Tarjan, and Francis Zane, “Resistance of Digital Watermarks to Collusive Attacks”, Technical Report TR-585-98, Department of Computer Science, Princeton University, 1998.では、統計的な議論によって文献[２]の電子透かし方式が何人までの結託者による結託攻撃に対する耐性を持っているかという理論的考察を行っている。疑似乱数系列はガウシアンノイズを仮定し、結託攻撃は結託者の持つコンテンツからオリジナルコンテンツを統計的に推定することで行うと仮定する。その結果、現実的なパラメータ設定で、数名から十数名の結託者に対する耐性を実現することが可能であるという結論が得られている。

【００５１】

また、電子透かしの応用形態によっては、オリジナルコンテンツを用いた検出が行えず、検出対象コンテンツのみから検出を行う必要がある場合がある。その場合には、類似度による検出は行えない。この場合には、許容される結託者の数はさらに小さくなると考えられる。

【００５２】

ところで、文献[２]や文献[１８]での議論は、すべて、符号語である擬似乱数列の間の相互相関が十分小さいという前提に基づいている。しかし、一般に擬似乱数列の数が増えてくると、仮にそれをランダムに選択したとしても、偶然に大きな相互相関値を持つ対が生ずる可能性が高くなってくると思われる。

【００５３】

いったい、どの程度多くの擬似乱数系列が任意の対の間で相互相関値を小さくできるのか、また、そのような性質を持つ擬似乱数列をどのように選択すれば良いのか、そして、そのようにして選択された擬似乱数列を符号語として、どのよ

うな電子透かし方式を実現すれば、結託攻撃に強い方式となるのかが未解決の問題として残されている。

【００５４】

この問題も、先に[結託攻撃耐性]の項で述べた文献[１７]での限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式をどう実現させるかという問題の一つと考えられる。

【００５５】

相互相関の小さな２値の擬似ランダムビット列を生成する方法として、M系列を利用する方法が知られている。M系列は、線形フィードバックシフトレジスタ(ＬＦＳＲ)の出力として得られる系列のうち、ＬＦＳＲがＧＦ(２)の原始多項式の係数に対応するタップを持つ場合に生成されるものである。M系列中の１と０をそれぞれ＋１と－１に置き換えると、ＰＮ系列となる。M系列は、０の出現頻度が１の出現頻度がほぼ等しく(１の出現頻度が一回少ない)、その間の相互相関関数は０のとき値１、０以外のとき－１／Ｌとなる。ここで、Ｌは系列の周期で、レジスタの段数をｎとすると、$L=2^{n}-1$である。

【００５６】

M系列から得られたＰＮ系列を巡回シフトして得られる系列を符号語として採用すれば、相互相関の小さな符号語が得られる。これらの符号語を電子透かしの埋め込みの際の擬似乱数系列として用いれば良い。この乱数系列は、空間領域利用型と周波数領域利用型の両方のスペクトラム拡散による電子透かしに利用できる。

【００５７】

周波数領域利用型のスペクトラム拡散の電子透かし方式では、普通、Ｎ(０，１)に従うガウシアンノイズを符号語とする。相互相関が小さな符号語を複数構成するには、逐次乱数列を生成し、それが、それまでに生成したすべての乱数列との相関が小さいことを確認し、仮に、大きな相互相関値を持つ場合には、その乱数列は符号語として採用しないという方法をとる。

【００５８】

しかし、この方法では、新たに生成した乱数列がそれまでに生成した乱数列と小さな相互相関であるという保証がないため、せっかく生成した乱数列を捨てなければならないことがあるため処理が無駄である。特に、乱数列の数がある程度以上増えると、その確率は高くなる。

【００５９】

【発明が解決しようとする課題】

以上に説明したように、従来の電子透かし技術では、結託攻撃によって透かし情報が失われたり偽造されたりすることで、不正な再配布が行われても、その不正行為者を特定できなくなる恐れがあった。

【００６０】

また、結託攻撃へのロバスト性を実現する従来の提案において、非常に冗長な形で透かし情報を埋め込む必要があるため、あまり大きな利用者総数や結託者数を想定することができないという欠点があった。

【００６１】

特に、ＪＰＥＧ圧縮等やその他の攻撃への耐性を持つ電子透かし埋め込み方式において、大きなサイズの透かし情報を埋め込むことはコンテンツの品質劣化を招く原因となる恐れがあった。

【００６２】

さらに、結託者特定の際の埋め込み符号の検出誤りを正しく評価した上で透かし情報(埋め込み符号)を構成する必要があるが、従来の電子透かし技術ではこのような点に対する考察、特に３人以上の結託者が改竄に関与した場合の対策が不十分であり、また検出誤りに対して必要以上に透かし情報である埋め込み符号の符号サイズを大きくしてしまう可能性があった。

【００６３】

本発明の目的は、結託攻撃への耐性を有し、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置及び電子透かし検出装置を提供することにある。

【００６４】

本発明の他の目的は、結託攻撃への耐性を有し、かつ３人以上の結託者が改竄

に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号検出装置を提供することにある。

【００６５】

【課題を解決するための手段】

上記の課題を解決するため、本発明に係る第１の埋め込み符号生成装置は、入力された利用者識別番号に対して、互いに素な複数の整数を法とする複数の剰余を求める剰余計算手段と、この剰余計算手段により求められた各剰余を表す符号であって、所定のビット数を一単位とする連続した１の列及び０の列で構成される複数の部分符号を生成する部分符号生成手段と、この記部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成する連接手段とを具備することを特徴とする。

【００６６】

この第１の埋め込み符号生成装置に対応する本発明に係る第１の埋め込み符号検出装置は、所定のビット数を一単位とする連続した１の列及び０の列で構成される複数の部分符号を連接した埋め込み符号を各部分符号に分割する符号分割手段と、分割された各部分符号をそれぞれ復号して予め定められた互いに素な複数の整数を法とする２つの剰余からなる複数の剰余対を得る部分符号復号手段と、前記複数の剰余対から結託者の利用者識別番号を計算する結託者番号計算手段とを具備することを特徴とする。

【００６７】

また、複数の剰余対から結託の有無を判定する結託判定手段をさらに有し、この結託判定手段により結託があると判定されたとき、結託者番号計算手段が結託者の利用者識別番号を計算するようにしてもよい。

【００６８】

結託者計算手段は、入力されたｋ′個の剰余対の各々から一方の剰余を選択してｋ′個の剰余の組（ｒ１，ｒ２，…，ｒｋ′）を生成する剰余選択部と、この剰余選択部により生成されたｋ′個の剰余の組からｋ個の剰余（ｒ１，ｒ２，…，ｒｋ）を選択する一貫性選択部と、この一貫性選択部により選択されたｋ個の剰

余から中国剰余定理に従って結託者の利用者識別番号ｕの候補を計算する中国剰余定理部とからなり、一貫性検査部は、中国剰余定理部により計算された結託者の利用者識別番号ｕの候補と残りの(ｋ′－ｋ)個の剰余のうちの所定個数(ｙ)の剰余との間にｒｉ＝ｕ ｍｏｄ ｐｉ(ｉ＝１，…，ｙ)が成立する場合があるか否かを判定し、この関係が成立する場合、ｕを結託の利用者識別番号として出力し、この関係が成立しない場合には剰余選択部に対して新たなｋ′個の剰余の組を要求し、結託者の利用者識別番号が特定できるまで新たな候補について同様の処理を繰り返す。

【００６９】

本発明に係る第２の埋め込み符号生成装置は、入力された利用者識別番号に対応して複数の整数要素の組を計算する計算手段と、所定個数の利用者識別番号に対して前記計算手段により計算される全ての整数要素の組を表現可能なｋ′個の部分符号のうちのｋ個の組み合わせが前記利用者識別番号を一意に表現できる部分符号を前記各整数要素に対応してそれぞれ生成する部分符号生成手段と、この部分符号生成手段により生成された各部分符号を連接して埋め込み符号を生成する連接手段とを具備し、前記ｋ′は、３以上の正整数をｃ、１以上の正整数を、前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数をｑとして、ｃ(ｋ＋１)／ｑ以上となるように決定されていることを特徴とし、より好ましくは前記所定個数の利用者識別番号に対して前記計算手段により計算される各整数要素のとり得る値をp_i(ｉ＝１，２，…，ｋ′)とし、前記埋め込み符号の検出時に想定される検出誤り率をεとしたとき、前記ｋ′は、

【００７０】

【数８】

$$\left[1-\prod_{i=1}^{l}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+1)/2C_{k+1}\times 2^{k+1}} \geq 1-\frac{\varepsilon}{2} \qquad (1)$$

【００７１】

の条件を満たすように設定されていることを特徴とする。

【００７２】

ここで、前記計算手段は、例えば入力された利用者識別番号に対応して互いに素な複数の整数を法とする剰余の組を前記整数要素の組として計算するか、あるいは入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算する。後者の場合、式(１)の条件に加え、前記p_i(ｉ＝１，２，…，ｋ′)を同一の正整数ｐとして、

【００７３】

【数９】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p-1} \qquad (2)$$

【００７４】

の条件をさらに満たすことを特徴とする。

【００７５】

第２の埋め込み符号生成装置に対応する本発明に係る第２の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なｋ′個の部分符号のうちのｋ個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各部分符号に分割する符号分割手段と、分割された各部分符号をそれぞれ復号する部分符号復号手段と、各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記ｋ′は、３以上の正整数をｃ、１以上の正整数を、前記埋め込み符号の検出時に前記各部分符号から検出できる前記整数要素の個数をｑとして、ｃ(ｋ＋１)／ｑ以上となるように決定されていることを特徴とし、より好ましくは前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値をp_i(ｉ＝１，２，…，ｋ′)とし、前記埋め込み符号の検出時に想定される検出誤り率をεとしたとき、前記ｋ′は、式(１)の条件を満たすように設定されていることを特徴とする。

【００７６】

ここで、前記整数要素の組は、例えば前記利用者識別番号に対応して計算された互いに素な複数の整数を法とする剰余の組、あるいは前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、後者の場合、式(１)の条件に加え、前記p_i(ｉ＝１，２，…，ｋ′)を同一の正整数ｐとして、式(２)の条件をさらに満たすことを特徴とする。

【００７７】

本発明に係る第３の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なｋ′個の部分符号のうちのｋ個の組み合わせが利用者識別番号を一意に表現できる部分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各部分符号に分割する符号分割手段と、分割された各部分符号をそれぞれ復号する部分符号復号手段と、各部分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記部分符号復号手段は、前記各部分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“１”のビット数を計数する計数部と、該計数部で得られた計数値が第１の閾値を越えているか否かを判定する第１の判定部と、前記計数値が第２の閾値に満たないか否かを判定する第２の判定部と、前記第１の判定部で第１の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第２の判定部で第２の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大値決定部の決定結果を復号結果として出力することを特徴とする。

【００７８】

さらに、本発明によると上述した第１または第２の埋め込み符号生成装置によって生成された埋め込み符号を埋め込み対象コンテンツに透かし情報として埋め込む電子透かし埋め込み装置が提供される。

【００７９】

本発明に係る他の電子透かし埋め込み装置は、埋め込み対象コンテンツに対し

て利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語を透かし情報として埋め込み対象コンテンツに埋め込む手段とを具備することを特徴とする。

【００８０】

本発明に係る他の電子透かし検出装置は、入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語とコンテンツとの相関値を求める手段と、この相関値に基づいてコンテンツ中の入力された利用者識別番号に対応する符号語の有無を判定する手段とを具備することを特徴とする。

【００８１】

このような本発明に基づく埋め込み符号生成装置／埋め込み符号復号装置及び電子透かし埋め込み／検出装置においては、透かし情報である埋め込み符号の符号サイズを大きくすることなく、利用者総数や結託者数が大きくなっても、結託攻撃に対するロバスト性を得ることができる。

【００８２】

また、$k' \geqq c(k+1)/q$以上という条件、さらには式(１)や式(２)の条件を満たすようにすることによって、３人以上の結託者が改竄に関与した場合においても、埋め込み符号検出時の正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号復号装置が実現される。

【００８３】

【発明の実施の形態】

図１は、本発明の電子透かし埋め込み装置１と電子透かし検出装置２が適用されるシステムの例であるフィンガープリンティングシステムの概念図を示す。

画像や音声などの埋め込み対象コンテンツと利用者識別番号が電子透かし埋め

込み装置１に入力され、ここで得られた埋め込み済みコンテンツがこれを格納する記憶媒体を含む流通経路３を経て流通する。

〔００８４〕

前述した結託攻撃は、流通経路３において埋め込みコンテンツに対して行われる。このような結託攻撃に対抗するために、本発明に基づく電子透かし検出装置２では、結託の有無を示す結託判定信号、結託があった場合の結託者を特定する結託者番号(結託者の利用者識別番号)、及び結託がなかった場合の正規の利用者識別番号が生成される。

〔００８５〕

以下、本発明による電子透かし埋め込み装置及び電子透かし検出装置の実施形態について説明する。

(第１の実施形態)

本発明の第１の実施形態として、従来例よりも小さな符号サイズを持つε誤りのc-secure符号による電子透かし埋め込み装置及び電子透かし検出装置について説明する。

図２は、本発明の第１の実施形態に係る電子透かし埋め込み装置の概略構成を示している。この電子透かし埋め込み装置は、埋め込むべき透かし情報である利用者識別番号の埋め込み符号を生成する埋め込み符号生成部１１と、生成された埋め込み符号を埋め込み対象コンテンツに埋め込み、埋め込み済みコンテンツを得る符号埋め込み部１２とからなる。

〔００８６〕

図３は、埋め込み符号生成部１１の構成を示している。この埋め込み符号生成部１１は、それぞれｋ′個の法記憶部２１－１，２１－２，…，２１－ｋ′、剰余計算部２２－１，２２－２，…，２２－ｋ′、部分符号生成部２４－１，２４－２，…，２４－ｋ′と、符号パラメータ記憶部２３及び符号連接部２５からなる。

〔００８７〕

法記憶部２１－１，２１－２，…，２１－ｋ′には互いに素な整数、この例では相異なるｋ′個の素数p_i(ｉ＝１，２，…，ｋ′)が法として記憶されており

、剰余計算部２２－１，２２－２，…，２２－ｋ′は、入力される利用者識別番号ｕに対して、これらの素数p_iを法とする剰余$u_i = u \bmod p_i$（ｉ＝１，２，…，ｋ′）をそれぞれ求める。すなわち、入力された利用者識別番号に対応した複数の整数要素の組として、剰余計算部２２－１，２２－２，…，２２－ｋ′により剰余$u_i = u \bmod p_i$（ｉ＝１，２，…，ｋ′）が計算される。

〔００８８〕

部分符号生成部２４－１，２４－２，…，２４－ｋ′は、ｋ′個の素数p_i（ｉ＝１，２，…，ｋ′）に対して、符号パラメータ記憶部２３に記憶された符号パラメータｄに従って剰余計算部２２－１，２２－２，…，２２－ｋ′により求められた剰余u_i（ｉ＝１，２，…，ｋ′）を表す前述した$\Gamma_0(n, d)$符号からなる部分符号$\Gamma(p_i, 1)$をそれぞれ生成する。すなわち、部分符号生成部２４－１，２４－２，…，２４－ｋ′では、所定個数（ｎ）の利用者識別番号に対して剰余計算部２２－１，２２－２，…，２２－ｋ′で計算される全ての剰余u_i（ｉ＝１，２，…，ｋ′）の組を表現可能なｋ′個の部分符号のうちのｋ個の組み合わせが利用者識別番号を一意に表現できる部分符号$\Gamma(p_i, 1)$を各剰余に対応して生成する。

〔００８９〕

符号連接部２５は、部分符号生成部２４－１，２４－２，…，２４－ｋ′により生成された各部分符号$\Gamma(p_i, 1)$を連接することによって、透かし情報である埋め込み符号を生成する。

〔００９０〕

図４に、部分符号生成部２４－１，２４－２，…，２４－ｋ′の一つ（２４－ｉ）の構成を示す。符号パラメータをｄ、剰余をu_i、法をp_iとすると、減算部３１では$p_i - u_i - 1$が求められる。“０”列生成部３２では、符号パラメータｄと剰余u_iに基づきｄ×u_iビットの連続した“０”列が生成され、“１”列生成部３３では、符号パラメータｄと減算部３１からの出力$p_i - u_i - 1$に基づきｄ×$(p_i - u_i - 1)$ビットの連続した“１”列が生成される。そして、これらの“０”列と“１”列が連接部３４で連接され、ｄ×$(p_i - 1)$ビットのビット列が$\Gamma_0(n, d)$符号からなる部分符号$\Gamma(p_i, 1)$として生成される。

〔００９１〕

図２０は、こうして生成される部分符号の一例を示している。０からｎ－１までのｎ個の利用者識別番号に対応して、Ｂ(０)，…，Ｂ(ｎ－２)のブロック“０”列からなる部分符号が割り当てられている。

〔００９２〕

図５に、本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、透かし情報抽出部４１、符号分割部４２、部分符号復号部４３－１，４３－２，…，４３－ｋ′、利用者識別番号計算部４４、結託判定部４５－１，４５－２，…，４５－ｋ′、結託判定ＯＲ部４６及び結託者番号計算部４７から構成されている。

〔００９３〕

透かし情報抽出部４１では、入力された埋め込み済みコンテンツから透かし情報(埋め込み符号)が抽出され、この抽出された透かし情報である埋め込み符号が符号分割部４２により各部分符号に分割された後、部分符号復号部４３－１，４３－２，…，４３－ｋ′により復号されることにより、利用者識別番号に対応する剰余対が生成される。

〔００９４〕

こうして生成された各剰余対の一方の剰余から、利用者識別番号計算部４４により利用者識別番号が計算で求められ、また各剰余対から結託判定部４５－１，４５－２，…，４５－ｋ′により結託の有無が判定される。結託判定部４５－１，４５－２，…，４５－ｋ′の判定結果について、結託判定ＯＲ部４６で論理和がとられることにより、結託が存在したか否かが最終的に判定される。さらに、結託が存在すると判定されたときは各剰余対から結託者番号計算部４７で結託者番号が計算され、結託者が特定される。

〔００９５〕

図６に、結託者番号計算部４７の詳細な構成を示す。この結託者番号計算部４７は、ｋ′個の剰余対から各一つの剰余を選択する剰余選択部５１と、選択されたｋ′個の剰余のうちｋ個の剰余を選択する一貫性検査部５２、及び一貫性検査部５２で選択されたｋ個の剰余に対して中国剰余定理を適用して結託者番号候補

を得る中国剰余定理部５３からなる。

〔００９６〕

図７に、図６中の一貫性検査部５２の内部構成を示す。中国剰余定理部５３により得られた結託者番号候補は一貫性検査部５２にフィードバックされ、ｋ′個の剰余のうち残りの(ｋ′－ｋ)個の剰余との間の一貫性検査が行われて、最終的に結託者番号が求められる。図７の一貫性検査部５２は、剰余の(ｋ＋１)組の生成部５２１と、剰余の１組と結託者番号候補の一貫性検査部５２２から構成される。その動作については、後に説明する。

〔００９７〕

本実施形態の電子透かし埋め込み装置及び電子透かし検出装置によると、利用者総数や結託者総数が大きい場合においても、コンテンツの品質劣化の少ない電子透かしが可能となる。以下、詳細に説明する。

利用者総数をｎとし、結託者総数の最大値をｃとする。一方、図３の法記憶部２１－１，２１－２，…，２１－ｋ′で用意されているｋ′個の素数ｐ1,ｐ2,…,ｐk′から任意のｋ個の素数を選んだとき、それらのｋ個の素数の積はｎ以上とする。例えば、この積は$n \leqq p_1 \times p_2 \times \cdots \times p_k$である。

〔００９８〕

埋め込み符号生成部１２では、各素数p_i(ｉ＝１，２，…ｋ′)に対して、図３の部分符号生成部２４－１，２４－２，…，２４－ｋ′により部分符号$\Gamma(p_i, 1)$が生成される。これらの部分符号$\Gamma(p_i, 1)$を符号連接部２５により連接することによって、新たな符号$\Gamma(p_1, p_2, \cdots, p_k' : 1)$が生成される。

〔００９９〕

ここで、各利用者の利用者識別番号をｕとすると、その利用者識別番号ｕに対応する連接符号$\Gamma(p_1, p_2, \cdots, p_k' : 1)$の符号語は、各部分符号$\Gamma(p_i, 1)$がその利用者識別番号ｕに対する素数$p_i$を法とする、剰余計算部２２－１，２２－２，…，２２－ｋ′で計算された剰余$u \bmod p_i$を表す符号語となり、これが透かし情報(埋め込み符号)として埋め込み対象コンテンツに埋め込まれることになる。

〔０１００〕

このようにして得られた埋め込み済みコンテンツに対して結託攻撃が行われた場合、図５の電子透かし検出装置において、符号分割部４２で分割された各部分符号$\Gamma(p_i, 1)$を部分符号復号部４３－１，４３－２，…，４３－ｋ′で復号することによって、ｃ人中のある２人の利用者識別番号のp_iに関する剰余(residue)の対が得られる。これをp_iに関する剰余対(residue pair)と呼ぶことにする。

〔０１０１〕

また、p_iに関する剰余対中のある剰余がある利用者識別番号ｕを保有する結託者の剰余であるとき、その剰余は利用者識別番号ｕを保有する結託者に起因すると呼ぶことにする。このとき、この結託者を含めて結託者と同じ剰余の値を持つ利用者に関しては、その剰余はその利用者の利用者識別番号に起因する可能性があると呼ぶことにする。

〔０１０２〕

（補題１）　ｃ人以下の結託において、$\Gamma(p_1, p_2, \cdots, p_{k'} : 1)$によりｋ′個の相異なる素数に関する剰余対が与えられたとき、それらの剰余対中に、ある結託者の利用者識別番号に起因する剰余の数が$2k'/c$以上含まれるような結託者が少なくとも１人存在する。

〔０１０３〕

（補題２）　剰余対中のある剰余に、結託により誤りを生じる確率をε以下とするには、$l \geqq \log_2(1/\varepsilon)$でなければならない。

〔０１０４〕

（系１）　ｋ′個の剰余対に含まれる剰余のどの一つの剰余にも、結託によって誤りが生じない確率をε以下とするには、$l \geqq \log_2(2k'/\varepsilon)$でなければならない。

〔０１０５〕

（補題３）　符号$\Gamma(p_1, p_2, \cdots, p_{k'} : 1)$は、結託により誤った符号を生じない確率をε以下とするには、$l \geqq \log_2(2k'/\varepsilon)$、つまり、符号サイズＬは、次式でなければならない。

〔０１０６〕

【数１０】

$$L \geq (\sum_{i=1}^{k'} pi) \times \log_2(2k'/\varepsilon) \qquad (3)$$

【０１０７】

以下、ｐｍ＝min(ｐ$_1$,…, ｐ$_{k'}$)、ｐＭ＝max(ｐ$_1$,…, ｐ$_{k'}$)とし、また

【数１１】

$$\langle P \rangle = \sum_{i=1}^{k'} pi/k' \qquad (4)$$

【０１０８】

とする。符号サイズの下限は、Ｌ＝ｋ′×＜ｐ＞×$\log^2$(２ｋ′／ε)と表わされる。

【０１０９】

(中国剰余定理(Chinese Remainder Theorem))

相異なるｋ個の素数ｐ$_1$,ｐ$_2$,…,ｐ$_k$が与えられたとき、各ｉ(ｉ＝１，２，…，ｋ)についてｕ$_i$∈Ｚｐｉが与えられると、ｕ$_i$≡ｕ mod ｐ$_i$であるｕ∈Ｚ$_{p1}$×Ｚ$_{p2}$×…×Ｚ$_{pk}$が一意に定まり、帰納的に計算できる。これが中国剰余定理である。

【０１１０】

中国剰余定理を適用すると、図６に示すように中国剰余定理部５３にｋ′個の素数のうちｋ個の素数に対応する剰余が与えられれば、それから利用者識別番号を一意に定めることができる。しかし、それらの剰余すべてが同一結託者の利用者識別番号に起因するとは限らないため、求めた利用者識別番号が結託者を正しく特定するとは限らない。

【０１１１】

そこで、さらに余分に１個の剰余を用意し、(ｋ＋１)個の剰余の間の一貫性を検査することで、得られた利用者識別番号の正当性を検証する。言い換えると、(ｋ＋１)個の連立合同方程式の解の存在を確認する。例えば、ｋ個の剰余から得

られた利用者識別番号に対して、残りの剰余r_{k+1}，…，r_{k+l}に対応する整数p_{k+1}，…，p_{k+l}で除した余り(remainder)を求め、それらがそれぞれ剰余r_{k+1}，…，r_{k+l}に一致し、一致したか否かで結託者を判定することとする。

【０１１２】

すなわち、図６の一貫性検査部５２では図７に示すように、図６の剰余選択部５１でｋ′個の剰余対から各一つ選択されたｋ′＝ｃ(ｋ＋１)／２個の剰余を剰余の(ｋ＋１)組の生成部５２１に入力し、これらｋ′個の剰余の中からｋ個の剰余を選択して中国剰余定理部５３に引き渡す。さらに、一貫性検査部５２２により剰余の１組と結託者番号候補との一貫性検査を行って、結託者番号(結託者の利用者識別番号)を出力する。

【０１１３】

結託者数が２人の場合については、この方法を比較的容易に実現できる(例えば、特願平１０－１０８０３９，特願平１０－１２２１０８)。ここでは、それを一般の結託者数に拡張する。

【０１１４】

ｍ個の素数に対応する剰余の組(m-tuple of residues)の中の任意のｋ個の剰余に対して中国剰余定理を適用したとき、これらｍ個の剰余の組がすべて同一の利用者識別番号を与える場合、このような剰余の組を一貫している(consistent)と呼ぶことにする。

【０１１５】

さらに、このような一貫している剰余の組の全ての剰余が、求められた結託者の利用者識別番号に起因している場合、この剰余の組は真に一貫している(truly consistent)と呼び、そうでない場合、この剰余の組は偽って一貫している(falsely consistent)と呼ぶことにする。このような偽って一貫している組の簡単な例を以下に挙げる。

一貫しているｍ個の剰余に対して、さらに第(ｍ＋１)番目の素数ｐに関する剰余を加えて(ｍ＋１)個の剰余としたとき、それらが一貫している確率は、新たに加えた素数ｐに関する剰余がランダムに値をとる場合には、１／ｐとなる。

【０１１６】

従って、ｍ個の剰余対から各１個の剰余を選択して、ｍ個の剰余を構成する場合、偶然に、偽って一貫したｍ個の剰余が得られる確率は、ｍを大きくするにつれて小さくなり、その確率は$(2/p_m)^{m-k}$より小さくなる。ただし、ｍ＞ｋとする。

〔０１１７〕

（系２） 偽って一貫した剰余の組が得られる確率をε以下とするには、$m \geqq k + \log_{p_m/2}(1/\varepsilon)$とすればよい。

ここで、系２から、偽って一貫した剰余の組が得られる確率をε以下とするためには、$m \geqq k + \log_{p_m/2}(1/\varepsilon)$個の同一利用者に起因する剰余を含む剰余対を用意すれば良い。（補題１）から、それには$k' \geqq (c/2) \times (k + \log_{p_m/2}(1/\varepsilon))$の剰余対を用意すれば良い。

〔０１１８〕

結託者を正しく決定するには、剰余対が正しく得られた上で真の一貫した組を得る必要がある。そこで、それぞれの誤り率εをε′と以下とすると、結託者を正しく決定できない確率は$(\varepsilon + \varepsilon')$以下となる。そこで、$\varepsilon \rightarrow \varepsilon/2$、$\varepsilon' \rightarrow \varepsilon/2$と再定義して、次の定理を得る。

〔０１１９〕

（定理１） 符号$\Gamma(p_1, p_2, \cdots, p_{k'} : 1)$が、誤り率ε以下で結託者を正しく決定するには、$k' \geqq (c/2) \times (k + \log_{p_m/2}(2/\varepsilon))$、$1 \geqq \log_2(4k'/\varepsilon)$を満たせば良い。

よって、（補題３）よりその符号サイズの下限は、

$$L = \langle p \rangle \times (c/2) \times (k + \log_{p_m/2}(2/\varepsilon)) \times \log_2((2c/\varepsilon) \times (k + \log_{p_m/2}(2/\varepsilon)))$$

で与えられる。

〔０１２０〕

ここで、すべての素数がほぼ同じ大きさとなるように選択する。$p_i \fallingdotseq p$とすると、$p \fallingdotseq \langle p \rangle \fallingdotseq n^{1/k}$。よって、符号サイズの下限は、

$$L \fallingdotseq (c/2) \times n^{1/k} \times (k + \log_{n^{1/k}/2}(2/\varepsilon)) \times \log_2((2c/\varepsilon) \times (k + \log_{n^{1/k}/2}(2/\varepsilon)))$$

で近似される。

〔０１２１〕

さらに、ある正数ａを選び、$k=(\log_2 n)/a$と設定することができるならば、符号サイズの下限は、

$$L \fallingdotseq (c e^a/2a)\times(\log_2 n + a\times\log_e a/2(2/\varepsilon)) \times\log_2((2c/\varepsilon a)\times(\log_2 n + a\times\log_e a/2(2/\varepsilon)))$$

で近似される。この場合、符号サイズの下限はｃに関して$\Theta(c\log_2 c)$、ｎに関して$\Theta(\log_2 n \log_2\log_2 n)$となり、例えば先の文献［１４］や文献［１５］に開示された従来の方式と比較して、最も小さなオーダーとなる。

(素数定理(prime number theorem))

自然数ｘを超えない素数の個数を$\pi(x)$とすると、$\pi(x)\fallingdotseq x/\log x$となる。先ほどの符号化では、$k=(\log_2 n)/a$とした。そこで、素数定理よりδを小さな正数とするとき、ｘ～ｘ(１＋δ)の間に素数が$\log_2 x$オーダーの個数以上存在することは、次のように確認できる。

〔０１２２〕

$$\pi(x+(1+\delta))-\pi(x)\fallingdotseq(x/(\log x-1)/\log^2 x) = \omega(\log x)$$

次に、上の定理１が前提としている、結託者を特定するアルゴリズムについて図８に示すフローチャートを用いて説明する。

結託者番号計算部４７は、部分符号復号部４３－１，４３－２，…，４３－ｋ′が出力したｋ′個の剰余対を入力する(ステップＳ１)。剰余対は、まず剰余選択部５１に入力される。剰余選択部５１は、各剰余対から一方の剰余を選択し、ｋ個の剰余の組(r_1, r_2, …, $r_{k'}$)を生成する(ステップＳ２)。

〔０１２３〕

生成されたｋ′個の剰余の組は、一貫性検査部５２に入力される。一貫性検査部５２は、入力されたｋ′個の剰余の組からｋ個の剰余(r_1, r2, …, r_k)を選択し(ステップＳ３)、中国剰余定理部５３に渡す。

〔０１２４〕

中国剰余定理部５３は、中国剰余定理に従い結託者番号ｕを計算する(ステッ

プＳ４)。この中国剰余定理の計算は、図９のフローチャートに示す処理の流れに従って行われる。計算された結託者番号ｕは、一貫性検査部５２へ返される。

〔０１２５〕

一貫性検査部５２では、残りの(ｋ′－ｋ)個の剰余のうちの所定個数(ｙ)の剰余との間に、$r_i = u \bmod p_i$ (ｉ＝１，…，ｙ)が成立する場合があるか否かを判定する(ステップＳ５)。この関係が成立する場合、一貫性検査部５２はｕを結託者番号として出力する(ステップＳ６)。この関係が成立しない場合には、一貫性検査部５２は剰余選択部５１に対して、新たなｋ′個の剰余の組を要求する(ステップＳ７)。もし、新たな候補が存在しない場合には、結託者番号の特定に失敗したことになる(ステップＳ８)。

〔０１２６〕

最後に、図１０に示すフローチャートを用いて本実施形態における電子透かし検出装置の処理の流れについて説明する。

埋め込み済みコンテンツが入力され(ステップＳ１１)、この埋め込み済みコンテンツから透かし情報抽出部４１で透かし情報である埋め込み符号が検出されると(ステップＳ１２)、符号分割部４２及び部分復号部４３－１，４３－２，…，４３ｋ′を介して得られた部分符号に基づいて、結託判定部４５－１，４５－２，…，４５－ｋ′により結託の有無が判定される(ステップＳ１３)。

〔０１２７〕

ここで、結託判定部４５－１，４５－２，…，４５－ｋ′のいずれでも結託が無いと判定されると、利用者識別番号計算部４４により利用者識別番号が計算され(ステップＳ１４)、この利用者識別番号が出力される(ステップＳ１５)。

〔０１２８〕

一方、ステップＳ１３で結託判定部４５－１，４５－２，…，４５－ｋ′の少なくとも一つで結託が有ると判定されると、結託判定部４６を介して結託存在信号が出力され(ステップＳ１６)、かつ結託者番号計算部４７で結託者番号が計算され(ステップＳ１７)、この結託者番号が出力される(ステップＳ１８)。

〔０１２９〕

この場合、ステップＳ１３での結託の有無の判定と、ステップＳ１４での利用

者識別番号の計算については、処理が簡単であり、高速に行うことができる。これに対して、ステップＳ１７での結託者番号の計算には時間がかかるが、結託の有無の判定を先に行い、結託が有ったと判断された場合にのみ結託者番号の計算を行うことにより、無駄な計算を省略できる。

【０１３０】

また、本発明の電子透かし検出装置を利用者機器に適用する場合には、結託の有無のみを判定し、その結果によって利用を中断させるなどの利用制御を行えばよいので、結託者の計算(特定)まで行う必要は必ずしもない。

【０１３１】

このように本実施形態によると、埋め込むべき符号サイズを抑えつつ、利用者総数や結託者数が大きい場合についても、結託攻撃に対するロバスト性を持つことができる。

【０１３２】

(第２の実施形態)

次に、上述した第１の実施形態を改良した本発明の第２の実施形態として、結託者特定の際の誤り率評価をより厳密にして必要な個数のみの素数を用意し、かつ符号サイズをより効果的に削減できる電子透かし埋め込み装置及び検出装置について説明する。

【０１３３】

第１の実施形態では、結託者の特定に際して埋め込み符号検出時の誤り評価を厳密に行っておらず、必ずしも用意すべき複数の素数(互いに素な整数)の個数の下限が正しく求められていない。また、用意すべき素数の個数が大きくなると、用意する最も小さな素数と比べて大きな素数まで用いる必要が生じるため、符号サイズ削減の効果が殺がれてしまう。第２の実施形態によると、このような課題を解決することができる。

【０１３４】

本実施形態に係る電子透かし埋め込み装置及び検出装置の構成は、第１の実施形態と基本的に同様であり、本実施形態では電子透かし埋め込み装置の部分符号生成部及び電子透かし検出装置の部分符号復号部として必要な個数(部分府古豪

の数)について述べる。

〔０１３５〕

利用者総数をｎとし、結託者の最大数をｃとする。先の文献[１３]によって導入されたε誤りを持つn-secure符号(cubic length n-secure code with ε-error)は、以下のように定義される。

〔０１３６〕

(定義１) ((ｎ－１)ｄ,ｎ)符号$\Gamma_0(n,d)$は、その符号語$w^{(0)},\cdots,w^{(n-1)}$が次の条件を満たす符号と定義する。

〔０１３７〕

〔数１２〕

$$w^{(i)}|_{B_j}=\begin{cases}\{0\}^d & \text{for } i>j\\ \{1\}^d & \text{otherwise}\end{cases} \qquad (5)$$

〔０１３８〕

ここで、$w^{(i)}|_{Bj}$は符号語$w^{(i)}$をビット位置の集合B_jに制限したものである。集合Ｂｉ, ｉ＝０,…,ｎ－２はブロック(blocks)と呼ばれ、ｄ個のビット位置から構成される。異なるブロック間は共通部分を持たない(ｉ≠ｊに対してＢｉ∩Ｂｊ＝φ)。

〔０１３９〕

すべての利用者に対して、シリアル番号のような形で順序をつけることができると仮定する。ｉ番目の利用者に対して、符号語$w^{(i)}$を割り当てるとする。さらに、利用者は自分に割り当てられたシリアル番号を知らされていないとする。

〔０１４０〕

先の文献[１２][１４]によって導入されたε誤りを持つ線形n-secure符号(linear length n-secure code with ε-error)は、符号語は定義１で定義された符号と同一であるが、検出アルゴリズムが異なる。この符号は、結託者中で最大と最小のシリアル番号をもつ２人の結託者を特定することができる。符号サイズは、Θ(n)である。

〔０１４１〕

(定理２)　以下の検出アルゴリズム１を符号$\Gamma_0(n,d)$に適用するとする。$d=\log_2(2/\varepsilon)$ならば、この符号はε誤りを持ったn-secure符号である。

〔０１４２〕

(検出アルゴリズム１)

(１)検出された符号$x\in\{0,1\}^l$を入力する。ここで、$l=(n-1)d$、$d=\log(1/\varepsilon)$とする。

(２)ｓ＝１からｎ－１まで、以下を実行する：

(２－１)もし、$x|_{Bs}\neq\{0\}^d$ならば中断する。

(３)ｔ＝ｎからｓまで、以下を実行する：

(３－１)もし、$x|_{Bi-1}\neq\{0\}^d$ならば中断する。

(４)ｓとｔを出力する。

〔０１４３〕

ｋ，ｋ′，ｌは、$k'=c(k+1)/2$を満足する正整数とする。$p_1,\cdots,p_{k'}$は、互いに素な整数とする。ｐは$p_1,\cdots,p_{k'}$のうち最小のものとする。また、$p_1,\cdots,p_{k'}$のうち小さい方から選んだｋ個の積をｎ以上とする。これらの整数$p_1,\cdots,p_{k'}$を以下では因数と呼ぶことにする。

〔０１４４〕

これらの因数の平均値をp_{ave}とする($p_{ave}=(p_1+\cdots+p_{k'})/k'$)。ｉ＝１,…,ｋ′の各$p_i$に対応して、先の文献［１３］のn-secure符号$\Gamma_0(p_i,t)$を構成要素の符号として用意する。

〔０１４５〕

(定義２)　$((p_{ave}-1)k'\ t,n)$符号$\Gamma(p_1\cdots,p_{k'};n,t)$は、その符号語$W^{(1)},\cdots,W^{(n)}$が次のように構成された符号であると定義する。

$$W^{(u)}|_{Ci}=w^{(u\bmod pi)}\in\Gamma_0(p_i,t)$$

ここで、C_iは構成要素の符号$\Gamma_0(p_i,t)$に対応するビット位置の集合である。この符号をｕ番目の利用者に割り当てることにする。

〔０１４６〕

埋め込み符号生成のための符号化アルゴリズムは、次の通りである。

(符号化アルゴリズム)

(１)利用者識別番号ｕ∈｛１,…,ｎ｝を入力する。

(２)ｉ＝１からｋ′まで以下を実行する：

(２－１)ｕ mod p_iを計算し、符号語ｗ(u mod pi)∈$\Gamma_0(p_i,t)$を生成する。

(３)生成された符号語を連接して、一つの符号語$W^{(u)}$とする。

この符号化アルゴリズムにより生成された埋め込み符号の検出アルゴリズムとしては、先の検出アルゴリズム１を利用する。

〔０１４７〕

(定義３)　Γ(ｐ1,…,ｐｋ′；ｎ，ｔ)の構成要素に対して、検出アルゴリズム１を適用することで、高々２つの整数$r_i^{(-)}, r_i^{(+)} \in Z_{p_i}$を得る。ここで、０≦$r_i^{(-)} \leqq r_i^{(+)} \leqq p_i$である。

これらの整数$r_i^{(-)}, r_i^{(+)} \in Z_{p_i}$を$\Gamma_0(p_i,t)$の剰余(residues)と呼ぶことにする。また、集合｛$r_i^{(-)}, r_i^{(+)}$｝を$\Gamma_0(p_i,t)$の剰余対(residue pair)と呼ぶことにする。

〔０１４８〕

(定義４)　ｒを$\Gamma_0(p_i,t)$の剰余とする。結託者の集合の中にｒ≡ｕ mod ｐｉを満たす結託者が存在する場合、剰余ｒはｕに起因する(r arises from u)と呼ぶ。また、利用者が結託者であるか否かに関わらず、ｒがｒ≡ｕ mod ｐｉを満足する場合、剰余ｒはｕに起因する可能性がある(possibly arise from)と呼ぶ。

〔０１４９〕

(検出アルゴリズム２)

(１)検出された符号ｘ∈$\{0,1\}^L$を入力する。ここで、Ｌ＝$(p_{ave}-1)k't$とする。

(２)ｘをｋ′個の制限$x|_{C_i}$，ｉ＝１,…,ｋ′個に分解する。

(３)ｉ＝１からｋ′まで以下を実行する：

(３－１)検出アルゴリズム１を$x|_{C_i}$に適用する。

(４)全ての剰余のｍ組に対して以下を実行する：

(４－１)もし、剰余のｍ組が一貫しているならば、以下を実行する：

（４－２）その解を結託者として出力し中止する。

（５）結託者が検出されなかったと出力する。

【０１５０】

（定理３）　$t \geqq \log_2(4k'/\varepsilon)$とする。以下の方程式が成立するとき、符号$\Gamma(p1,\cdots,pk';t)$はε誤りを持ったc-secure符号である。

【０１５１】

【数１３】

$$\left[1-\left\{1-\left(1-\frac{1}{p}\right)^{c}\right\}^{l}\right]^{t\cdot C_{k+1}\cdot 2^{k+1}} > 1-\frac{\varepsilon}{2} \qquad (6)$$

【０１５２】

このとき、符号サイズは、$L=(p_{ave}-1)k't$で与えられる。

【０１５３】

（補題４）　符号$\Gamma(p1,\cdots,pk';n,t)$のk′個の剰余対の中には、少なくとも$2k'/c$個の剰余を起因させている結託者が少なくとも１人存在する。

（補題４の証明）　符号$\Gamma(p1,\cdots,pk';n,t)$のk′個の剰余対に含まれる剰余は$2k'$個ある。平均すると、結託者１人あたり$2k'/c$個の剰余を起因させていることになる。従って、少なくとも1人の結託者は、$2k'/c$個以上の剰余を起因させている。

【０１５４】

（補題４の一般化）

補題４は、各部分符号から検出できる整数要素（剰余）の個数qをq＝２とした場合の例であるが、これをqを用いて一般化すると、次の通りとなる。

【０１５５】

（一般化した補題４の証明）

符号$\Gamma(p1,\cdots,pk';n,t)$のk′個の剰余q対（対ではないが、ここでは便宜上、そう呼ぶことにする）に含まれる剰余は、qk'個ある。平均すると結託者１人あたり、qk'/c個の剰余を起因させていることになる。従って、少なくとも１人の結託者は、qk'/c個以上の剰余を起因させている。

〔０１５６〕

ここで、結託者番号(結託者の利用者識別番号)の再構成と検定には、(ｋ＋１)個の剰余が必要なので、一般化した補題４の結果より、ｑｋ′／ｃ≧ｋ＋１が成立する必要がある。左辺の因子ｑ／ｃを右辺に移すと、条件式ｋ′≧ｃ(ｋ＋１)／ｑを得る。

〔０１５７〕

(補題５)　$t \geqq \log_2(2k'/\varepsilon)$とする。符号Γ(ｐ1,…,ｐｋ′;ｎ, ｔ)に対して先の検出アルゴリズム１を適用するとき、ｋ′個の剰余対の検出誤り率(ｋ′個の剰余対の中に、どの結託者にも起因しない剰余が含まれてしまう確率)は、εε以下である。

〔０１５８〕

(補題５の証明)　ある構成要素Γ_0(ｐｉ,ｔ)に対して検出アルゴリズム１を適用するときは、定理２より$t \geqq \log_2(2k'/\varepsilon)$ならば、剰余対の検出誤り率はε／ｋ′以下である。全部でｋ′個の構成要素が存在するので、全ての剰余対に対する検出誤り率はε以下である。

(補題６)　ある一貫した剰余のｍ組が存在しており、これに別の因数ｑに対する剰余対からの剰余を加えて剰余の(ｍ＋１)組を構成するとき、この(ｍ＋１)組の剰余が偽に一貫している確率は、$1-(1-1/q)^c$以下である。

〔０１５９〕

(補題６の証明)　各剰余対は、全ての結託者の利用者識別番号に対するｑを法とする剰余のうちの最大値と最小値により構成されている。利用者は自分の利用者識別番号を知らないので、結託が行われたとき、ある利用者識別番号が結託者のものである確率は、利用者識別番号によらず一様であると考えられる。従って、ある結託者の剰余がある値をとる確率は、等しく１／ｑである。

〔０１６０〕

ｃ人の結託者の剰余が全て一様に分布するとき、最大の剰余がある値$c \in Z_q$をとる確率Ｐｒ[ｘ]は、以下のように与えられる。

〔０１６１〕

【数１４】

$$\Pr[x]=\begin{cases}\left(1-\dfrac{x}{q}\right)^{c}-\left(1-\dfrac{x+1}{q}\right)^{c} & \text{for } x=q-1\\ \left(\dfrac{1}{q}\right)^{c} & \text{for } x=q-1\end{cases} \qquad (7)$$

【０１６２】

(補題７)　以下の条件が成り立つとき、偽に一貫している剰余の(ｋ＋１)組が存在する確率は次式に示すようにε以下である。

【０１６３】

【数１５】

$$\left[1-\left\{1-(1-1/p)^{c}\right\}^{l}\right]^{c(k+1)/2C_{k+1}\times 2^{k+1}}>1-\varepsilon \qquad (8)$$

【０１６４】

(補題７の証明)　　ｋ′個の剰余対から剰余の(ｋ＋１)組を選択する組合せは、$_{k'}C_{k+1}\times 2^{k+1}$通りある。補題１４から、剰余の(ｋ＋１)組が偽に一貫している確率は、$(1-(1-1/q)^{c})^{l}$である。従って、全ての組合せにおいて、少なくとも1個の偽に一貫している剰余の(ｋ＋１)組が現れる確率は、次のような上限が与えられる。

【０１６５】

【数１６】

$$P_F\le 1-\left[1-\left\{1-(1-1/p)^{c}\right\}^{l}\right]^{k'C_{k+1}\times 2^{k+1}} \qquad (9)$$

【０１６６】

補題４の条件式が成立するとき、確率P_Fはε以下である。

〔０１６７〕

（定理３の証明） 潔白な利用者を誤って結託者であると検出する原因は、剰余対の検出誤りと偽に一貫している剰余の組の選択の二つがある。それぞれの確率をε／２以下とするならば、検出誤り率はε以下となる。補題５と補題７より、上の上限の式を得る。

偽に一貫している剰余の組を排除する確率を最小の因数で下限を抑える代わりに、小さい方から１個の因数を用いて下限を抑えることで、式(６)に代えて次式に示すような符号サイズのより小さな上限を得ることができる。

〔０１６８〕

〔数１７〕

$$\left[1-\prod_{i=1}^{l}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+1)/2C_{k+1}\times 2^{k+1}} \geq 1-\frac{\varepsilon}{2} \qquad (10)$$

〔０１６９〕

ここで、p_1, …, p_lはp_1, …, $p_{k'}$の中から選んだ１個(ただし、$p_1<p_2\cdots<p_l$とする)であり、最も小さいものから順に選んだ１個であってもよいし、ｋ＋１番目から小さい順に最も大きいｋ＋１番目まで選んだ１個であってもよいし、あるいは最も小さいものからｋ＋１番目に小さいものまでの中から選んだ１個であってもよい。また、p_i(ｉ＝１，２，…，ｋ′)はｃ個の利用者識別番号に対して剰余計算部で計算される各剰余（整数要素）のとりうる値であり、本実施形態では前述の法記憶部２１－１，２１－２，…，２１－ｋ′で用意されているｋ′個の素数である。

〔０１７０〕

式(１０)の意味について説明する。まず、式(１０)の左辺は、検出が正しく結託者番号を特定する確率の下限を与えている。つまり、左辺の大括弧の肩に乗っている「べき」は、ｋ′個の剰余対から(ｋ＋１)個の剰余を選択してくる場合の例である。その個々の選択に対して、結託者番号が正しいか否かの判定を正しく

行う確率の加減が右辺全体の意味するところである。

【０１７１】

ここで、式(１０)左辺の大括弧の中身について詳しく説明する。上記の各選択では、結託者番号が正しいか否かを余分に１個の剰余によって検定している。大括弧の中のΠによる積の部分は、１個の検定すべてが、誤った結託者番号を正しいとしてしまう確率の上限を与えている。なぜなら、各検定が誤った結託者番号を正しいと判定してしまう確率の下限は、(補題６)において、与えている確率１－(１－１／ｑ)^{c}において、各部分符号から検出できる整数要素（剰余）の個数ｑ（本実施形態ではｑ＝２）をその剰余に対応する因数で置き換えたものによって与えられる。

【０１７２】

検定に用いられる剰余に対応する１個の因数は、最も小さな因数からなる組み合わせがp_1, p_2, …, p_lの場合であって、この組み合わせが、誤った検定を行う確率の下限を最大にする組み合わせである。よって、Πによる積部分が１個の検定すべてが、誤った結託者番号を正しいとしてしまう確率の上限を与えていることになる。よって、式(１０)は左辺であるところの正しい結託者番号を検出する確率の下限が右辺であるところの１－ε／２以上であるための条件式を意味していることになる。

【０１７３】

このように本実施形態によると、前述した一般化した補題４によって与えられる条件式ｋ′≧(ｋ＋１)／ｑを満たすように、より好ましくは式(１０)を満足するように部分符号の数ｋ′を規定することによって、結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することができる。

【０１７４】

(第３の実施形態)

次に、本発明の第３の実施形態として、ある条件の下で実現できる、第２の実施形態よりも短い符号サイズのc-secure符号による電子透かし埋め込み装置及び

検出装置について説明する。

【０１７５】

図１１は、本実施形態に係る電子透かし埋め込み装置における埋め込み符号生成部の構成を示すブロック図である。この埋め込み符号生成部は、利用者識別番号を入力して同値類に基づく部分符号を生成する部分符号生成部６１－１，６１－２，…，６１－ｋ′と、これらの各部分符号を一つの符号に連接することによって、透かし情報である埋め込み符号を生成する符号連接部６２からなる。

【０１７６】

図１２に、図１１の同値類に基づく部分符号生成部６１－１，６１－２，…，６１－ｋ′の一つ(６１－ｉ)の構成を示す。以下、$Z_p=\{0, 1, 2, \cdots, p-1\}$とする。部分符号生成部６１－ｉは、$Z_p^k$内対応点計算部６１１と同値類要素番号計算部６１２及び部分符号生成部６１３によって構成される。

【０１７７】

Z_p^k内対応点計算部６１１は、利用者識別番号を入力して、対応するZ_p^k内の点を出力する。利用者識別番号ＩＤ(ｕ)とZ_p^k内の点$(u_0, u_1, u_2, \cdots, u_{p-1})$との対応付けは、例えば、$u=u_0+u_1p+\cdots+u_{k-1}p^{k-1}$によって行う。ある集合Ｕの要素に間に同値関係Ｒがあるとき、その同値関係Ｒによってある要素ｕと同値なもの全体の集合をその要素ｕの同値類と呼ぶ。Ｕの同値関係Ｒに関する同値類全体からなる集合をＵ／Ｒで表し、ＵのＲに関する同値類という。Z_p^kの要素の間にある平行移動Ｔによって、同値関係R_Tが定義できる。そして、この同値関係R_Tに関する同値類が定義できる。

【０１７８】

一つの同値類に属する要素に対して、０から$p^{k-1}-1$まで番号(これを同値類要素番号と呼ぶことにする)を割り振ることができる。同値類要素番号計算部６１２は、この同値類番号を計算して部分ＩＤとして出力する。すなわち、本実施形態では入力された利用者識別番号に対する整数要素の組として、同値類要素番号計算部６１２により同値類要素番号が計算される。部分符号生成部６１３は、同値類要素番号計算部６１２で計算された部分ＩＤから部分符号を生成する。

【０１７９】

図１３は、平行移動による同値類の例を示す図である。これはｐ＝７，ｋ＝２の例である。平行移動(１，６)と平行移動(３，４)は、斜線部で示される格子によって構成されている同じ同値類を定義していることが分かる。

〔０１８０〕

図１４は、図１３のｐ×ｐの格子を周期的に繰り返したとき、同値類がどのように表されるかを示す図である。平行移動による同値関係によって定義される同値類であって、(０，０)の格子を含む同値類は、ある傾きを持った直線上に乗っていることが分かる。図１５は、図１４をｋ＝３に拡張した場合の例を示す図である。同様にして、任意の正整数ｋに対して平行移動による同値関係によって同値類を定義することができる。

〔０１８１〕

一つの同値類に含まれる元の個数は、ｐ個である。順序番号(同値類内要素番号)は、このｐ個の元に対して与えられる。

一方、商集合の要素の個数(＝同値類の個数)は$p^k/p=p^k-1$である。従って、順序番号を指定すると、p^k-1個の元が指定されることになる。この順序番号が部分ＩＤとして部分符号によって符号化されることになる。

〔０１８２〕

ここで、同値類要素番号計算部６１２での同値類要素番号(部分ＩＤ)の割当て方法について述べる。この割当て方法として、次の２通りが考えられる。

〔０１８３〕

(割当て方法１)　同値関係R_Aに関する同値類に対して割り当てた番号である同値類番号を用いる方法であり、０から$p^{k-1}-1$までの番号が割り当てられる。

〔０１８４〕

(割当て方法２)　同値類の要素に対して割り当てた番号を用いる方法であり、０からｐ－１までの番号が割り当てられる。

〔０１８５〕

これらのうち割当て方法２がより好ましい。この割当て方法１を採用した場合には、第２の実施形態と同様の議論が展開できるため、先の式(６)が成立する。

つまり、式(６)と後述する式(２７)の両者を満足するような符号を採用すれば良い。この割当て　　方法２の例を挙げる。平行移動$A_i=(a_{i,0},a_{i,1},\cdots,a_{i,k-1})$による同値類の場合、$u=(u_0,\cdots,u_{k-1})$は、同値類要素番号(部分ＩＤ)として次式が割り当てられる。

【０１８６】

【数１８】

$$\sum_{j=0}^{k-1} u_j a_{i,j} \bmod p \qquad (11)$$

【０１８７】

図１６に、本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、透かし情報抽出部７１、符号分割部７２、同値類に基づく部分符号復号部７３－１，７３－２，…，７３－ｋ′及び結託者番号計算部７４から構成されている。

【０１８８】

透かし情報抽出部７１では、入力された埋め込み済みコンテンツから透かし情報(埋め込み符号)が抽出され、この抽出された透かし情報である埋め込み符号が符号分割部７２により各部分符号に分割された後、同値類に基づく部分符号復号部７３－１，７３－２，…，７３－ｋ′により復号されることにより、利用者識別番号に対応する同値類要素番号の対が生成される。こうして生成された各同値類要素番号の対から、結託者番号計算部７４で結託者番号が計算され、結託者が特定される。

【０１８９】

なお、第１、第２の実施形態と同様に、同値類要素番号の対の一方から利用者識別番号計算部により利用者識別番号を計算で求め、また各同値類要素番号の対から結託判定部により結託の有無を判定し、その結託判定部判定結果について、結託判定ＯＲ部で論理和をとることにより、結託が存在したか否かを最終的に判定して、結託が存在すると判定されたときに結託者番号計算部７４で結託者番号を計算する構成としてもよい。

〔０１９０〕

図１７は、同値類に基づく部分符号復号部７３－１，７３－２，…，７３－ｋ′の一つ(７３－ｉ)の構成を示している。同値類に基づく部分復号部７３－ｉは、後述するランダム誤りを許容する検出アルゴリズム３に基づくものであり、ブロック分割部７３０、“１”ビット計数部７３１、“＞t_0”判定部７３２、“＜$d-t_0$”判定部７３３、最小位置決定部７３４及び最大位置決定部７３５から構成される。

〔０１９１〕

ブロック分割部７３０は、入力された部分符号を各ブロックへ制限したものに分割して分割結果をそれぞれ“１”ビット計数部７３１へ出力する。“１”ビット計数部７３１は、“１”が立っているビットの数を計数して、その計数値を“＞t_0”判定部７３２及び“＜$d-t_0$”判定部７３３へそれぞれ出力する。

〔０１９２〕

“＞t_0”判定部７３２は、入力が第１の閾値t_0より大きいか否かを判定し、真ならば１、偽ならば０をそれぞれ出力する。“＜$d-t_0$”判定部７３３は、入力が第２の閾値ｄ－ｔ0より小さいか否かを判定し、真ならば１、偽ならば０をそれぞれ出力する。

〔０１９３〕

最小位置決定部７３４は、“＞t_0”判定部７３２からの入力ビットの組のうち１が立っている最小のビット番号を出力する。最大位置決定部７３５は、“＜$d-t_0$”判定部７３３からの入力ビットの組のうち１が立っている最大のビット番号を出力する。

〔０１９４〕

ここで、図１６の電子透かし検出装置において埋め込み符号である透かし情報の復号時に誤りが生ずる可能性がある場合について説明する。埋め込み符号の復号時に誤りがある場合には、誤った利用者を結託者と特定するおそれがある。この誤りを防ぐには２通りの方法がある。

〔０１９５〕

（方法１） 電子透かし埋め込み装置において、埋め込み符号に対して誤り訂正

符号化を行ってから埋め込みを行い、電子透かし検出装置において検出された符号に対して誤り訂正復号を行う。

（方法２） 図１６の部分符号復号部７３－１，７３－２，…，７３－ｋ′に誤りを許容する性質を持たせる。

【０１９６】

本実施形態では、（方法２）を採用する。抽出された埋め込み符号には誤り確率のランダムな誤りが加わっていると仮定する。第２の実施形態で述べた検出アルゴリズム１に改良を加えた以下のような検出アルゴリズム３を用いることで、誤りを許容する。

【０１９７】

（検出アルゴリズム３）

（１）検出された符号$x \in \{0,1\}^{l}$を入力する。ここで、ｌ＝（ｎ－１）ｄとする。

（２）ｓ＝０からｎ－２まで、以下を実行する：

（２－１）もし、$\mathrm{weight}(x|_{Bs})>0$ならば、中断する。

（３）ｔ＝ｎ－１からｓまで、以下を実行する：

（３－１）もし、$\mathrm{weight}(x|_{Bl-1})<d-t_0$ならば、中断する。

（４）ｓとｔを出力する。

ここでt_0は、この検出アルゴリズム３の誤りに対する許容性を表すパラメータである。

【０１９８】

次に、結託による埋め込み符号の改竄があったことを判定する閾値として、新たなパラメータを加える意味について説明する。

埋め込み符号のうち、結託によっては改竄んが行われなかったブロックに対して、結託以外の原因でランダムな誤りが発生した場合、t_0+1ビット以上の反転が生ずる確率は、次式で与えられる。

【０１９９】

【数１９】

$$\varepsilon_1 = \sum_{i=t_0+1}^{d} {}_d C_i (1-\varepsilon_0)^{d-i} \varepsilon_0{}^i < e^{-\frac{(t_0-d\varepsilon_0)^2}{d}} \qquad (12)$$

【０２００】

一方、結託によって改竄が行われたブロックに対して、結託以外の原因でランダムな誤りが加法的に加わった場合、t_0ビット以下の反転が生ずる確率は、次式より小さい。

【０２０１】

【数２０】

$$\varepsilon_2 = \sum_{i=0}^{t_0} {}_d C_i (1/2)^d < e^{-\frac{\left(\frac{d}{2}-t_0\right)^2}{d}} \qquad (13)$$

【０２０２】

ランダム誤りのために埋め込み符号を誤って検出をしてしまう確率は、少なくとも一つのブロックにおいて誤った検出をする確率以下であり、この確率は、

$\varepsilon_3 = 1-(1-\varepsilon_1)^{n-1}(1-\varepsilon_2)^2 < (n-1)\varepsilon_1 + 2\varepsilon_2$

で表される。図１８に示すようにt_0を適当に選択することで、加法的にランダムな誤りが加わった場合にも、検出誤りを小さく設定できる。

図１７に示した部分符号復号部７３－ｉは、上述したようなランダム誤りを許容する先の検出アルゴリズム３に基づく処理を行う。

【０２０３】

図１９に、結託者番号計算部７４の構成を示す。結託者番号計算部７４は、同値類選択部８１、一貫性検査部８２及び候補ＩＤ計算部８３から構成される。

【０２０４】

同値類要素選択部８１は、ｋ′個の同値類要素番号の対の各々から一方の同値類番号を選択して一貫性検査部８２へ出力し、一貫性検査部８２から次候補の要

求を受けると、同値類要素番号の新たな組を選択する。

〔０２０５〕

一貫性検査部８２は、ｋ′個の組から（ｋ＋１）個の組を選択し、その同値類要素番号の組が真に一貫しているか否かを検査する。この検査は、（ｋ＋１）個のうちｋ個の同値類要素番号を候補ＩＤ計算部８３に渡し、返された候補ＩＤが残りの同値類要素番号の示す同値類番号と矛盾していないか否かを判定することにより行われる。残りの個のすべての同値類番号に対して、この判定が矛盾していないという結果ならば、この候補ＩＤを結託者番号として出力し、そうでない場合には、次候補を一貫性検査部８２に要求する。

〔０２０６〕

ここで、図１９中の候補ＩＤ計算部８３においてｋ個の同値類要素番号から結託者番号を再構成する方法を示す。例えば、ｋ個の平行移動$A_{i(0)}$，…，$A_{i(k-1)}$に対して、同値類要素番号がr_0，…，r_{k-1}で与えられた場合、次式の連立合同方程式が成り立つ。

〔０２０７〕

〔数２１〕

$$\sum_{j=0}^{k-1} u_j a_{i(v),j} \equiv r_v \bmod p \qquad (14)$$

〔０２０８〕

ｋ次正方行列$(a_{i(v),j})$が正則ならば、逆行列$(a^{-1}_{j,i(v)})$が存在する。この場合、次式によって利用者識別番号が得られる。

〔０２０９〕

〔数２２〕

$$u_j \equiv \sum_{v=0}^{k-1} a^{-1}{}_{j,i(v)} r_v \bmod p \qquad (15)$$

〔０２１０〕

一般には、正則性が満たされるとは限らない。正則性が満足されない場合には

、利用者識別番号は一意に決まらず、結託者番号を含む利用者識別番号の集合が得られる。この集合は、ｐのべき乗の大きさを持つ。正則性を満たさない部分符号の組はあらかじめ分かっているので、結託者ＩＤの候補の計算には、選択しないような構成もできる。

〔０２１１〕

図１９中の一貫性検査部８２は、こうして得られた結託者番号の候補(を含む集合に対して)と、さらに１個の同値類要素番号r_k，…，r_{k+l-1}との間の一貫性を検証する。それは、ｖ＝０，…，１－１に対して、次式が成立することを確認することで行われる。

〔０２１２〕

〔数２３〕

$$\sum_{j=0}^{k-1} u_j a_{i(k+v),j} \equiv r_{k+v} \bmod p \qquad (16)$$

〔０２１３〕

本実施形態によると、第２の実施形態と同様に結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することが可能となる。以下、詳細に説明する。

〔０２１４〕

まず、ｐを正整数とする。すなわち、本実施形態では第２の実施形態におけるp_i(ｉ＝１，２，…，ｋ′)(所定個数ｎの利用者識別番号に対して計算される剰余の値の個数)に相当する個数（所定個数ｎの利用者識別番号に対して計算される整数要素の値の個数）を同一の正整数ｐとしている。そして、利用者識別番号ｕを$u=u_0+u_1p+\cdots u_{k-1}p^{k-1}$に従って、$(u_0,u_1,\cdots,u_{k-1})\in Z_p^{\,k}$で表現する。また、$k'=c(k+1)/2$とし、$p^k \geqq n$とする。

〔０２１５〕

空間$Z_p^{\,k}$の平行移動$A\equiv(a_0,a_1,\cdots,a_{k-1})$に関する同値関係$R_A$を以下のように定義する。

〔０２１６〕

$R_A((u_0, u_1, \cdots, u_{k-1}),((u_0', u_1', \cdots, u_{k-1}'))$

$\longleftrightarrow$ $u_0' \equiv u_0 + a_0 \bmod p$,

$u_1' \equiv u_1 + a_1 \bmod p \cdots$,

$u_{k-1}' \equiv u_{k-1} + a_{k-1} \bmod p$

$jA-(ja_0 \bmod p, ja_1 \bmod p, \cdots, ja_{k-1} \bmod p)$とすると、ｊがgcd(ｊ，ｐ)＝１を満たすときには、R_AとR_{jA}とは同じ同値関係を与える。

〔０２１７〕

利用者全体の集合を$U=Z_p{}^k$の同値関係R_Aに関する商集合U/R_Aが定義できる。この商集合の個々の元は同値類と呼ばれ、同値関係R_Aによって同一視された元の集合である。すべての同値類に対して、それに含まれる元に順序番号を与えることにより、ある番号を指定することで、各同値類から１個ずつ元を選択できる。

〔０２１８〕

ｋ′（ｋ′≧ｋ）個の平行移動$A_0, \cdots, A_{k'-1}$を用意すると、それぞれに対して商集合$Q_i=U/R_{Ai}$（ｉ＝０，…，ｋ′－１）が定義される。各商集合に対して、上に述べた順序番号を定義する。

〔０２１９〕

次に、ｋ′個の商集合中の任意のｋ個の商集合のそれぞれに対して、順序番号を指定することで、利用者を一意に特定できるような商集合の組を構成するために、以下のような条件を仮定する。

〔０２２０〕

（条件１）　商集合の大きさを等しいとする。すべての$A_i=(a_{i,0}, \cdots, a_{i,k-1})$（ｉ＝０，…，ｋ′－１）において、すべての$a_{i,m}$（ｍ＝０，…，ｋ－１）に対して、$\gcd(a_{i,m}, p)=1$または$a_{i,m}=0$であるとする。これにより、$jA_i=(0 \bmod p, \cdots, 0 \bmod p)$を満たす最小の正整数ｊはｐとなる。

（条件２）　２つの平行移動Ａｉ，A_i'に対して、$jA_i=j'A_i'$が成立する正整数ｊ＜ｐ，ｊ′＜ｐが存在しない。

ｐが素数の場合、このような条件を満たす平行移動の個数は、次のように数え

上げることができる。

まず、(条件１)より各平行移動の成分の値がｐと互いに素である場合の数は、$\phi(p)=p-1$で表される。ここで、ϕはオイラー関数である。これに０である場合を加えて、各成分がとりうる値の場合の数は、ｐである。従って、平行移動として許される場合の数は、(p^k-1)個である。ここで、－１は、(０,０,…,０)を除外したことによる。ところが、これらの中には$(p-1)$個ずつ互いに他の整数倍(１倍、２倍、…、$(p-1)$倍)となっているものがある。従って、実際に、相異なる商集合を定義する平行移動として独立なものは、$(p^k-1)/(p-1)$個となる。

【０２２１】

また、(条件２)に関しては、仮にある２つの平行移動Ａｉ,A_i'が(条件２)の制約を満たさないとする。つまり、正整数ｊ＜ｐ,ｊ′＜ｐに対してｊＡｉ＝ｊ′A_i'とすると、ｐが素数の場合には、これは互いに他の整数倍で表現できることを意味する。よって、(条件１)に対して数え上げた独立な平行移動は、そのまま(条件２)を満足する。

平行移動の組は、次のように具体的に構成できる。

【０２２２】

【数２４】

$$\begin{aligned}
A_1 &= (0,0,\cdots,0,1),\\
A_2 &= (0,0,\cdots,0,1,0),\\
&\vdots\\
A_{1+p} &= (0,0,\cdots,0,1,p-1),\\
A_{1+p+1} &= (0,0,\cdots,0,1,0,0),\\
&\vdots\\
A_{1+p+p^2} &= (0,0,\cdots,0,1,p-1,p-1),\\
&\vdots\\
A_{1+p+p^2+\cdots+p^{t-2}+1} &= (1,0,\cdots,0),\\
&\vdots\\
A_{1+p+p^2+\cdots+p^{t-1}} &= (1,p-1,\cdots,p-1).
\end{aligned} \qquad (17)$$

【０２２３】

ｐが素数でない場合についても、(条件１)(条件２)を満足するように平行移動

を選択すれば、同様の構成が可能である。

【０２２４】

上述したような平行移動の組によって商集合を構成し、各商集合の同値類の元に順序番号を定義することで、中国剰余定理に基づく符号の場合と同様の符号を構成できる。この符号が誤りεを持つc-secure符号となるためには、定理３が成立することに加えて、以下の条件が満たされなければならない。

【０２２５】

【数２５】

$$k' = \frac{c}{2}(k+l) \leq \frac{p^k - 1}{p-1} \qquad (18)$$

【０２２６】

この場合、全ての因数は同じ大きさのｐであるので、p_{ave}＝ｐである。

【０２２７】

このように本実施形態によると、部分符号として式(１７)で示されるような平行移動によって定義される同値類に基づく符号を生成して、この部分符号を連接することで、第１、第２の実施形態よりも短い符号サイズのc-secure符号による埋め込み符号を生成し、その埋め込み符号を検出する場合において、第２の実施形態で規定した条件式ｋ′≧ｃ（ｋ＋１）／ｑや式(１０)の条件に加え、さらに式(２７)の条件を満足するようにすることによって、結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することができる。

【０２２８】

（第４の実施形態）

次に、本発明の第４の実施形態として、埋め込み済みコンテンツの品質への影響を小さく抑えるように、従来よりも最適な符号化が行われる電子透かし埋め込み装置及び検出装置について説明する。

【０２２９】

図２２に、本実施形態に係る電子透かし埋め込み装置の構成を示す。この電子透かし埋め込み装置は、シンプレックス符号生成部９１、符号語選択部９２及び電子透かし埋め込み部９３から構成されている。

【０２３０】

シンプレックス符号とは、符号長ｎ－１、符号語数ｎで、符号語間の相互相関が－１／(ｎ－１)となる符号であり、ｎ次のアダマール(Hadamard)行列を基に構成することができる。すなわち、符号語がｎ－１次元ユークリッド空間中のｎ－１次元単体の頂点に位置するような符号がシンプレックス符号である。例えば、３次元ユークリッド空間の場合は、図２１に示すように(-1,-1,1)，(1,-1,-1)，(-1,1,-1)で示す３つの頂点に位置する符号がシンプレックス符号を構成する。

【０２３１】

シンプレックス符号生成部９１では、このようなシンプレックス符号の符号語を生成する。シンプレックス符号生成部９１は、あらかじめ生成された符号語の表を記憶したものであってもよい。符号語選択部９２は、生成されたシンプレックス符号に順番を割り振っておき、与えられた利用者識別番号に対応する符号語を選択して出力する。なお、シンプレックス符号生成部９１及び符号語選択部９２の部分は、利用者識別番号が入力されてから、利用者識別番号に対応するシンプレックス符号の符号語を生成して出力するように構成されていてもよい。

【０２３２】

電子透かし埋め込み部９３は、符号語選択部９２より受け取った符号語を透かし情報として埋め込み対象コンテンツに埋め込む。埋め込みは、スペクトラム拡散によって行う。

【０２３３】

図２３に、図２２に示した電子透かし埋め込み装置に対応する本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、シンプレックス符号生成部１０１、符号語選択部１０２、相関値計算部１０３及び相関値判定部１０４から構成されている。シンプレックス符号生成部１０１と符号語選択部１０２については、図２２で説明した電子透かし埋め込み装置の中のそれと同一であるため、説明を省略する。

【０２３４】

相関値計算部１０３では、入力された埋め込み済みコンテンツと入力された利用者識別番号に基づいて符号選択部１０２で選択された符号語との間の相関値を計算する。相関値判定部１０４では、相関値計算部１０３により計算された相関値がある閾値を超えているか否かによって、符号選択部１０２からの符号語が埋め込み済みコンテンツに埋め込まれているか否かを判定し、検出／非検出信号を出力する。

【０２３５】

このように本実施形態に係る電子透かし埋め込み／検出装置によれば、任意の対の間での相互相関値が小さくなるようなシンプレックス符号の符号語を擬似乱数系列として用い、これを透かし情報として埋め込んでいる。従って、透かし情報として別の利用者識別番号に対応する符号語が埋め込まれていると誤判定を行う確率は非常に小さくなる。

【０２３６】

（第５の実施形態）

次に、本発明の第５の実施形態として、第４の実施形態の電子透かし検出装置を応用して結託攻撃に対する結託者特定機能を持たせた電子透かし検出装置ついて説明する。図２４は、本実施形態に係る結託者特定機能に係る部分の構成を示している。

【０２３７】

この電子透かし検出装置は、結託者特定機能を持たせるために、シンプレックス符号生成部１１１、符号語選択部１１２、相関値計算部１１３、利用者識別番号生成部１１４、相関値ベクトルノルム計算部１１５、電子透かし判定部１１６及び結託者判定部１１７を有する。シンプレックス符号生成部１１１、符号語選択部１１２及び相関値計算部１１３は、図２３に示した電子透かし検出装置の中のそれと基本的に同じである。

【０２３８】

利用者識別番号生成部１１４では、予め登録されたすべての利用者識別番号を生成する。符号語選択部１１２では、これらすべての利用者識別番号に対応する

シンプレックス符号の符号語が選択され、これらの各符号語と図示しない埋め込み済みコンテンツとの相関値が相関値計算部１１３で計算される。

【０２３９】

相関値ベクトルノルム計算部１１５では、すべての利用者識別番号に対して計算された相関値をベクトルとみなして、そのノルムを計算する。この相関値ベクトルノルムは、例えばすべての相関値の和とする。

【０２４０】

電子透かし判定部１１６では、計算されたベクトルノルムに基づいて、例えば、このノルムがある閾値を超えるか否かにより、透かし情報が埋め込まれていたか否かを判定する。この判定の結果、透かし情報が埋め込まれていたと判断した場合には、結託者判定部１１７において相関値ベクトルの中で最も大きな値を示した利用者識別番号を保有する利用者を結託者として特定する。

【０２４１】

また、結託者特定部１１７においては、このような方法の他、例えば相関値ベクトルがｎ－１次元単体の部分単体のうち、どの部分単体の重心を通るかを求め、その部分単体の頂点に対応する利用者識別番号を保有する利用者を結託者とすることで、複数の結託者を特定することもできる。

【０２４２】

なお、第４乃至第５の実施形態において、透かし情報として用いる擬似乱数系列として、Ｎ(０，１)のガウシアンノイズを採用する場合には、図２５に示すようにシンプレックス符号生成部１２１で生成されたシンプレックス符号をランダム座標回転部１２２によりランダムに回転させて符号語とすればよい。

【０２４３】

さらに、本発明に係る埋め込み符号生成装置は、電子透かし埋め込み装置のようにディジタルデータである埋め込み対象コンテンツの透かし情報として埋め込むための埋め込み符号のみでなく、例えば化学物質からなる合成物などに化学的に埋め込むための埋め込み符号を生成するような用途にも適用できる。

【０２４４】

【発明の効果】

以上説明したように、本発明によればフィンガープリンティングシステムを構成する電子透かし埋め込み／検出装置において、利用者総数や結託者数が大きくなっても、小さな符号サイズの透かし情報を埋め込ことによってコンテンツの品質劣化を伴うことなく、結託攻撃に対するロバスト性を持つことができ、非可逆圧縮等の他の攻撃に対してもロバスト性を得ることができる。

【０２４５】

また、本発明の電子透かし埋め込み／検出装置により、コピー制御情報や利用制御情報といった透かし情報を埋め込み、コンテンツを利用する機器を制御する場合に、同一コンテンツに対して異なる機器制御情報が埋め込まれている場合にその比較によって制御情報の改竄を行う攻撃に対してもロバスト性を有するコンテンツ利用システムを構築することも可能である。

【０２４６】

さらに、本発明によると結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号検出装置を提供することができる。

【図面の簡単な説明】

【図１】　本発明に係る電子透かし埋め込み装置及び電子透かし検出装置が適用されるフィンガープリンティングシステムの概略構成を示す図

【図２】　本発明の第１の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図３】　図２における埋め込み符号生成部の構成を示すブロック図

【図４】　図３における部分符号生成部の構成を示すブロック図

【図５】　本発明の第１の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図６】　図５における結託者番号計算部の構成を示すブロック図

【図７】　図６における一貫性検査部の構成を示すブロック図

【図８】　同実施形態における結託者特定アルゴリズムを示すフローチャート

【図９】　図５における中国剰余定理部の処理の流れを示すフローチャート

【図１０】　同実施形態に係る電子透かし検出装置の処理の流れを示すフローチャート

【図１１】　本発明の第３の実施形態に係る埋め込み符号生成部の構成を示すブロック図

【図１２】　図１１における同値類に基づく部分符号生成部の構成を示すブロック図

【図１３】　同実施形態における平行移動による同値類によって商集合が定義できることを示す図

【図１４】　同実施形態における平行移動による同値類の例を示す図

【図１５】　同実施形態におけるｋ＝３の場合の同値類の例を示す図

【図１６】　同実施形態に係る電子透かし検出装置の構成を示すブロック図

【図１７】　図１６における同値類に基づく部分符号復号部の構成を示すブロック図

【図１８】　図１７に示した同値類に基づく部分符号復号部について説明する図

【図１９】　図１６における結託者番号計算部の構成を示すブロック図

【図２０】　本発明で生成される部分符号(結託前の部分符号)の値を示す図

【図２１】　本発明の第４乃至第５の実施形態で使用するシンプレックス符号について説明する図

【図２２】　本発明の第４の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図２３】　本発明の第４の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図２４】　本発明の第５の実施形態に係る結託者特定機能を有する電子透かし検出装置の構成を示すブロック図

【図２５】　本発明の第４乃至第５の実施形態におけるシンプレックス符号生成部の他の例を示すブロック図

【図２６】　電子透かしに対する結託攻撃について説明する図

【図２７】　$\Gamma_0(n, d)$符号及びそれに対する結託攻撃を説明する図

【図２８】　$\Gamma_0(n, d)$符号における二つの符号間の最大距離と最小距離について説明する図

【図２９】　$\Gamma_0(n, d)$符号を用いた従来の電子透かしアルゴリズムにおける問題点を説明する図

【符号の説明】

１１…埋め込み符号生成部

１２…符号埋め込み部

２１－１，２１－２，…，２１－ｋ′…法記憶部

２２－１，２２－２，…，２２－ｋ′…剰余計算部

２３…符号パラメータ記憶部

２４－１，２４－１，…，２４－ｋ′…部分符号生成部

２５…符号連接部

４１…透かし情報抽出部

４２…符号分割部

４３－１，４３－２，…，４３－ｋ′…部分符号復号部

４４…利用者識別番号計算部

４５－１，４５－２，…，４５－ｋ′…結託判定部

４６…結託判定ＯＲ部

４７…結託者番号計算部

５１…剰余選択部

５２…一貫性検査部

５３…中国剰余定理部

６１－１，６１－２，…，６１－ｋ′…同値類に基づく部分符号生成部

６２…符号連接部

７１…透かし情報抽出部

７２…符号分割部

７３－１，７３－２，…，７３－ｋ′…同値類に基づく部分符号復号部

７４…結託者番号計算部

８１…同値類選択部

８２…一貫性検査部

８３…候補ＩＤ計算部

９１…シンプレックス符号生成部

９２…符号語選択部

９３…電子透かし埋め込み部

１０１…シンプレックス符号生成部

１０２…符号語選択部

１０３…相関値計算部

１０４…相関値判定部

１１１…シンプレックス符号生成部

１１２…符号語選択部

１１３…相関値計算部

１１４…利用者識別番号生成部

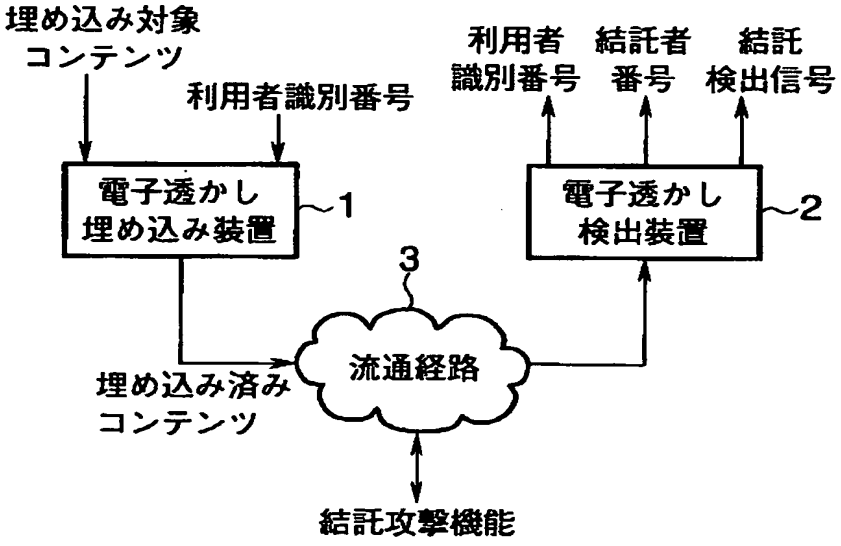
１１５…相関値ベクトルノルム計算部

１１６…電子透かし判定部

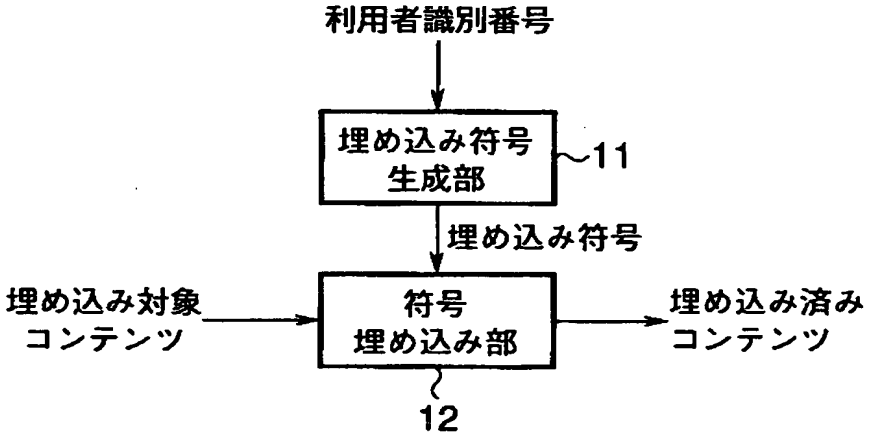
１１７…結託者特定部

【書類名】　　図面

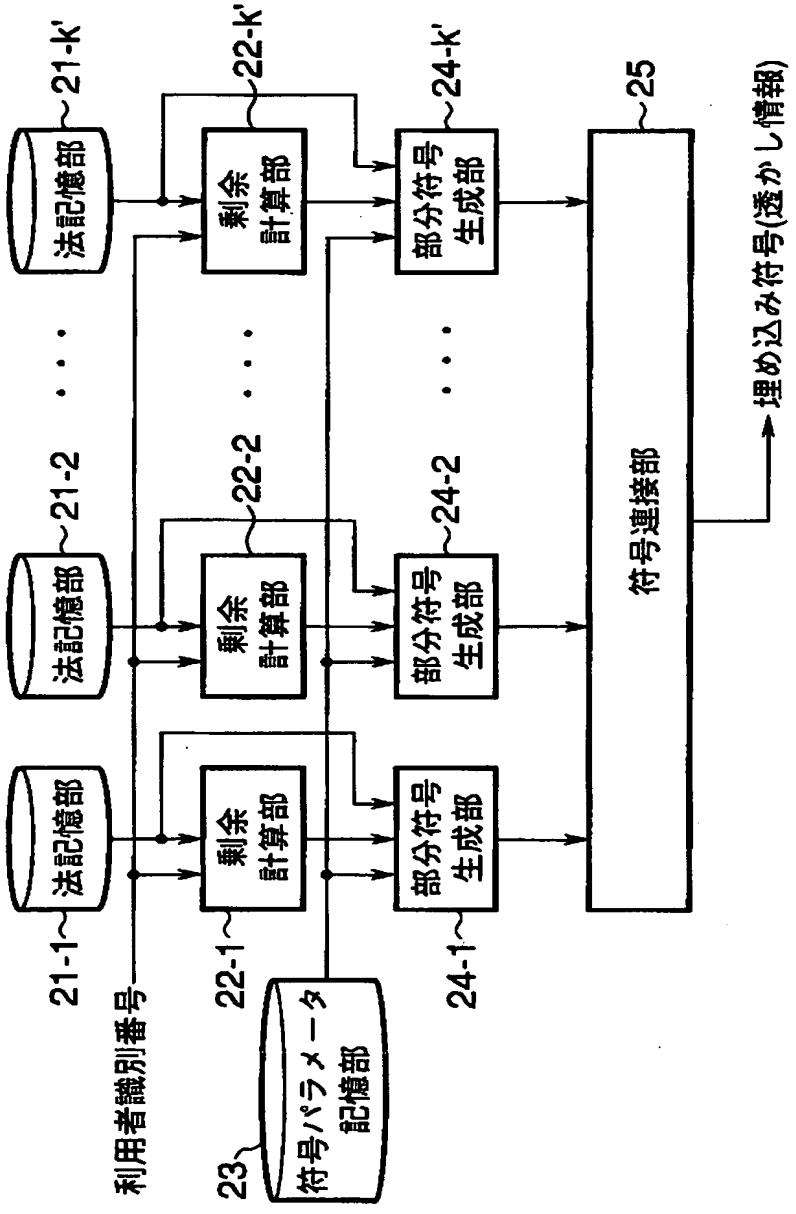
【図１】


埋め込み対象
コンテンツ
利用者識別番号
利用者
識別番号
結託者
番号
結託
検出信号
電子透かし
埋め込み装置
1
電子透かし
検出装置
2
3
流通経路
埋め込み済み
コンテンツ
結託攻撃機能

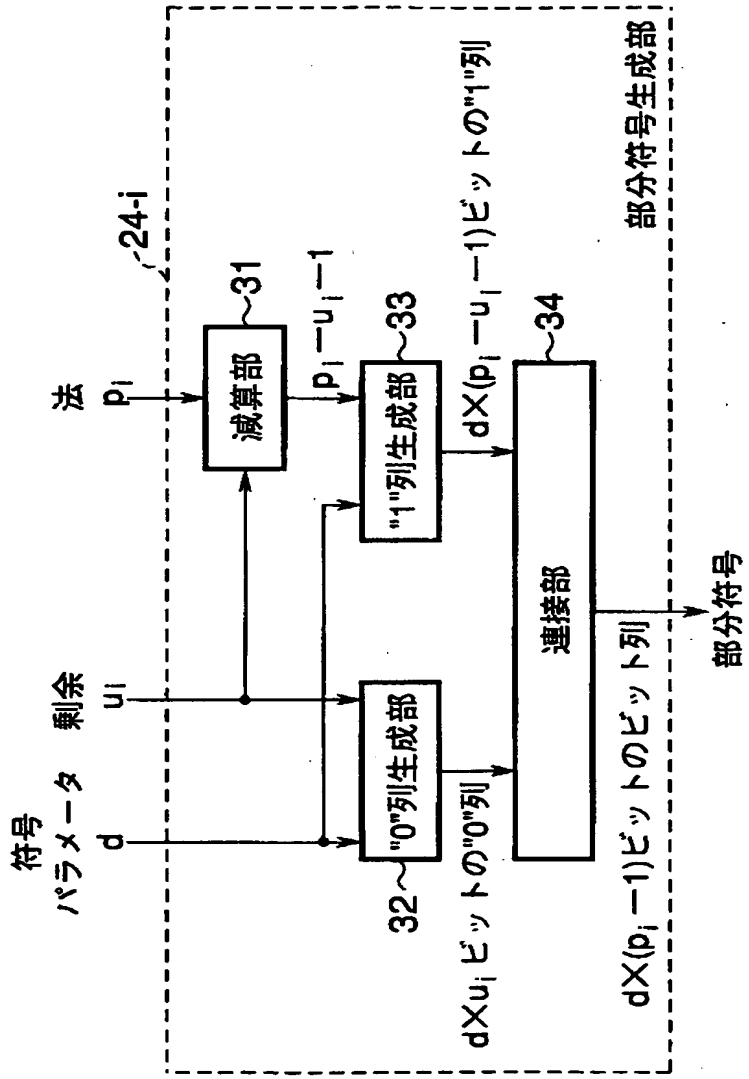
【図２】


利用者識別番号
埋め込み符号
生成部
11
埋め込み符号
埋め込み対象
コンテンツ
符号
埋め込み部
埋め込み済み
コンテンツ
12

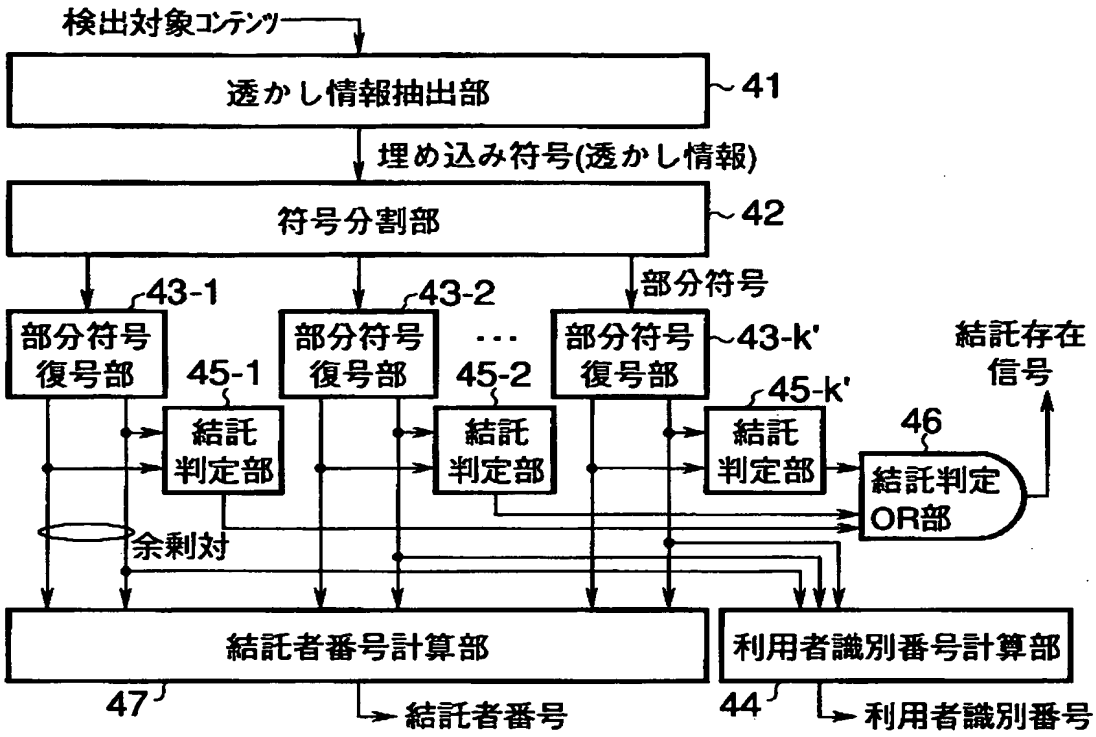
【図３】


21-k'
22-k'
24-k'
25
法記憶部
剰余計算部
部分符号生成部
符号連接部
埋め込み符号(透かし情報)
21-2
22-2
24-2
21-1
22-1
24-1
利用者識別番号
23
符号パラメータ記憶部

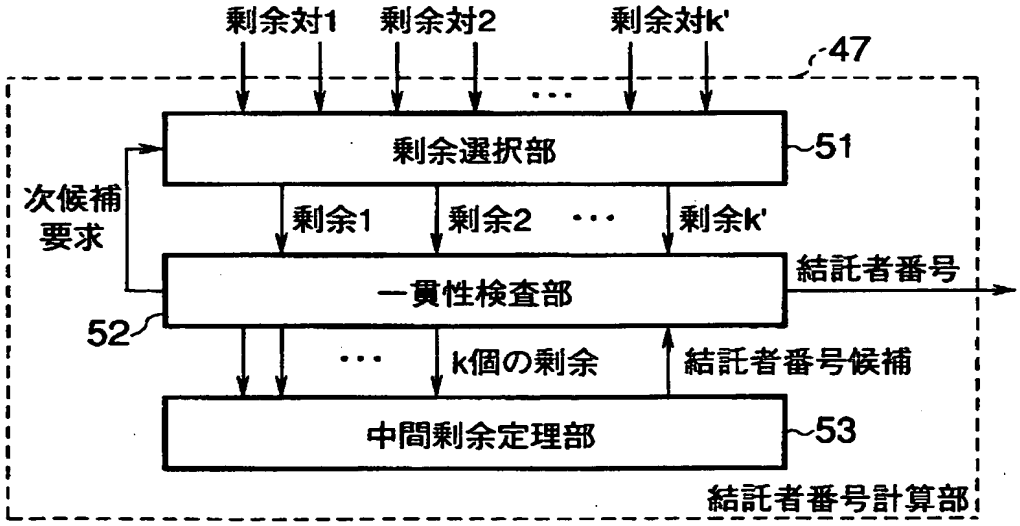
【図４】


符号
パラメータ
剰余法
d
ui
pi
24-i
減算部
31
pi−ui−1
"0"列生成部
32
"1"列生成部
33
dXui ビットの"0"列
dX(pi−ui−1)ビットの"1"列
連接部
34
dX(pi−1)ビットのビット列
部分符号生成部
部分符号

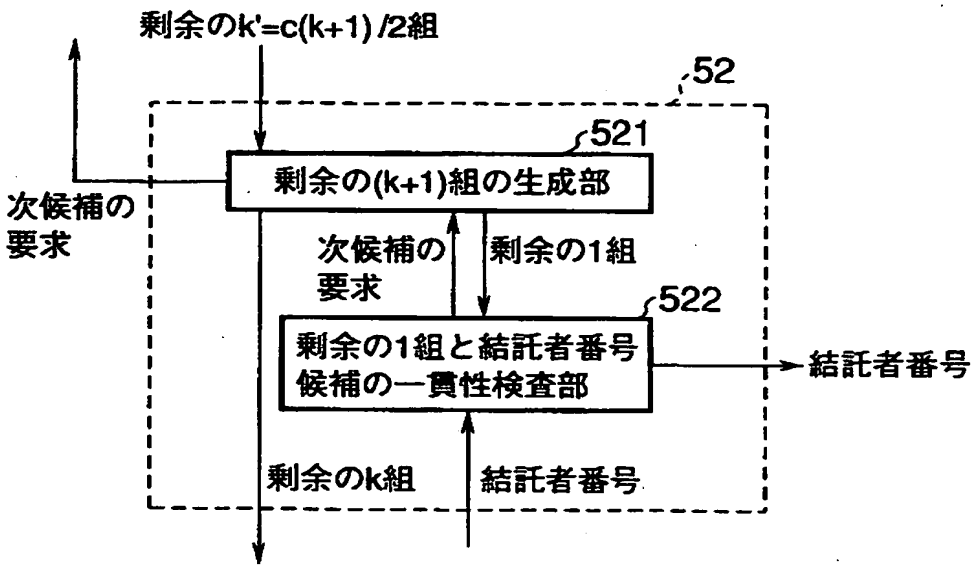
【図５】


検出対象コンテンツ
透かし情報抽出部
41
埋め込み符号(透かし情報)
符号分割部
42
部分符号
43-1
43-2
43-k'
部分符号復号部
45-1
45-2
45-k'
結託判定部
結託存在信号
46
結託判定OR部
余剰対
結託者番号計算部
47
結託者番号
利用者識別番号計算部
44
利用者識別番号

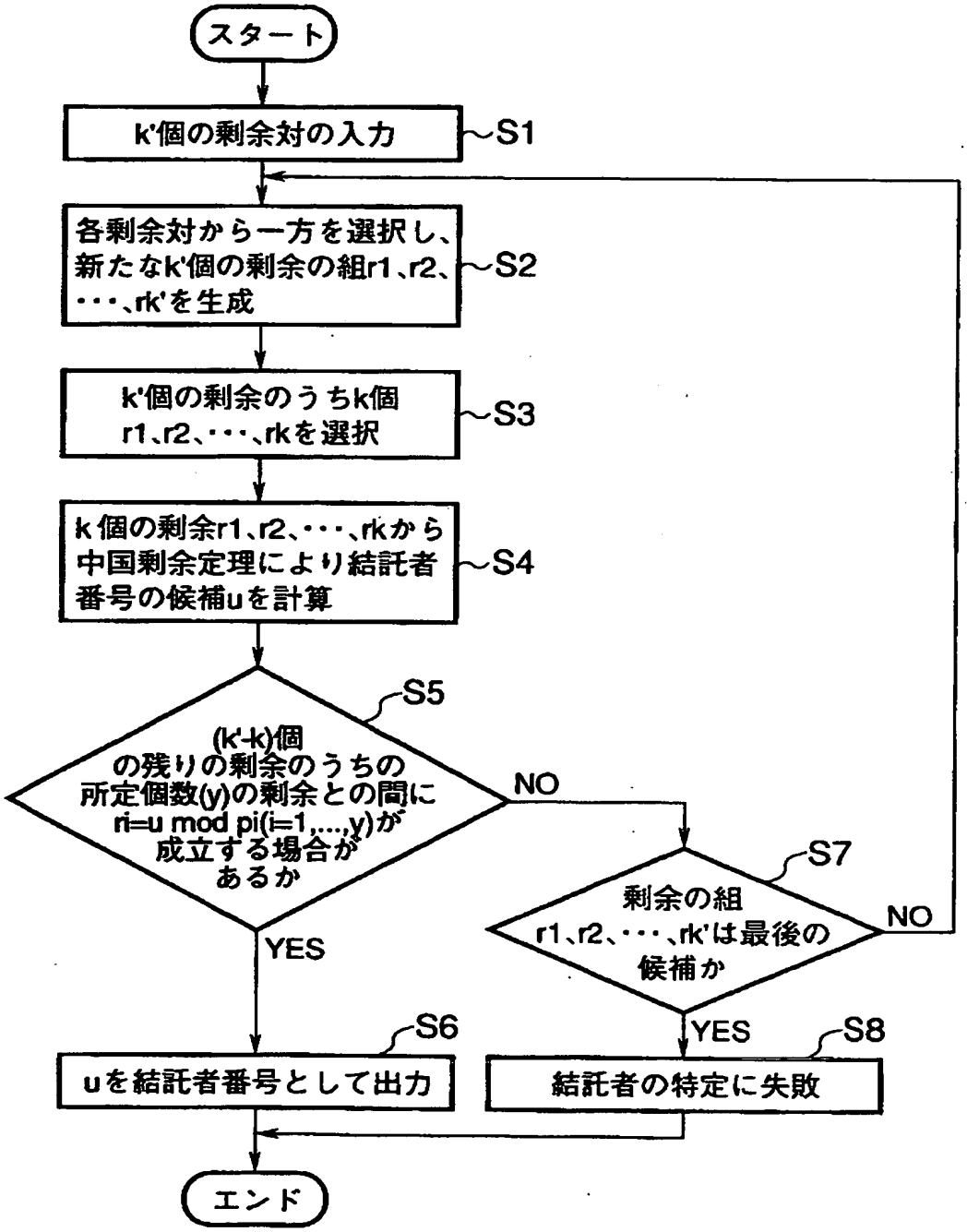
【図６】


剰余対1
剰余対2
剰余対k'
47
剰余選択部
51
次候補要求
剰余1
剰余2
剰余k'
一貫性検査部
結託者番号
52
k個の剰余
結託者番号候補
中間剰余定理部
53
結託者番号計算部

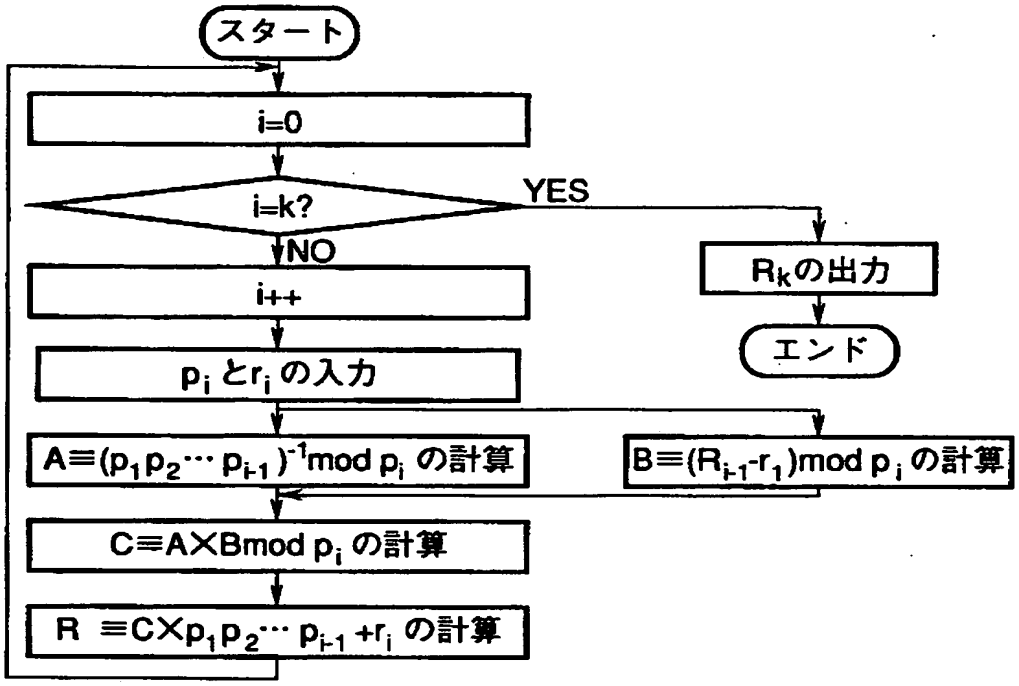
【図７】


剰余のk'=c(k+1)/2組
52
521
剰余の(k+1)組の生成部
次候補の
要求
次候補の
要求
剰余の1組
522
剰余の1組と結託者番号
候補の一貫性検査部
結託者番号
剰余のk組
結託者番号

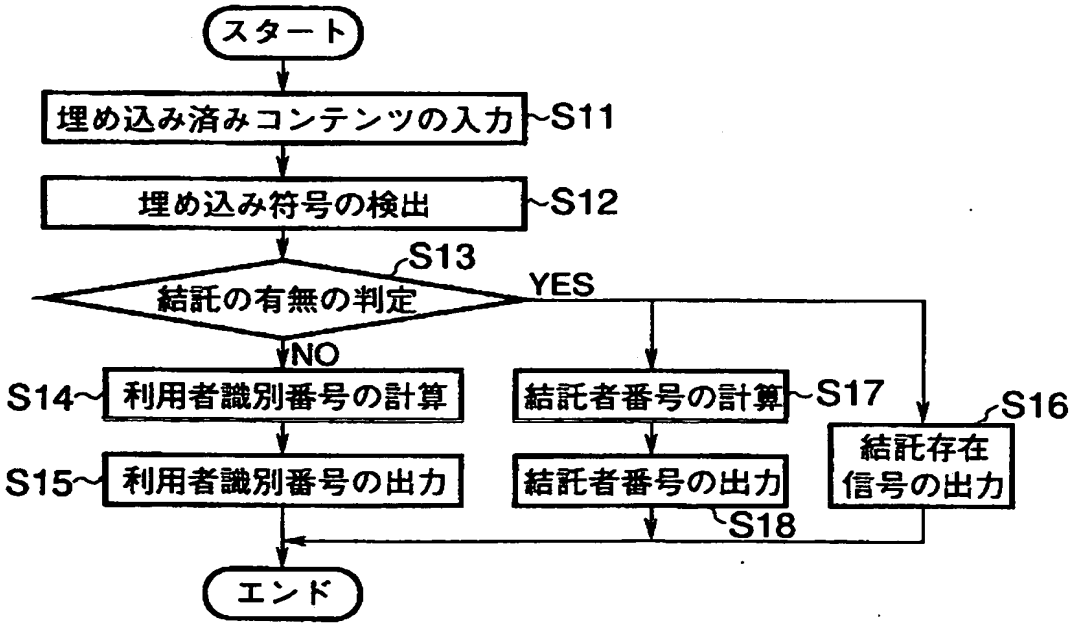
【図８】


スタート
k'個の剰余対の入力
S1
各剰余対から一方を選択し、新たなk'個の剰余の組r1、r2、・・・、rk'を生成
S2
k'個の剰余のうちk個r1、r2、・・・、rkを選択
S3
k個の剰余r1、r2、・・・、rkから中国剰余定理により結託者番号の候補uを計算
S4
S5
(k'-k)個の残りの剰余のうちの所定個数(y)の剰余との間にri=u mod pi(i=1,...,y)が成立する場合があるか
NO
YES
S7
剰余の組r1、r2、・・・、rk'は最後の候補か
NO
YES
S6
uを結託者番号として出力
S8
結託者の特定に失敗
エンド

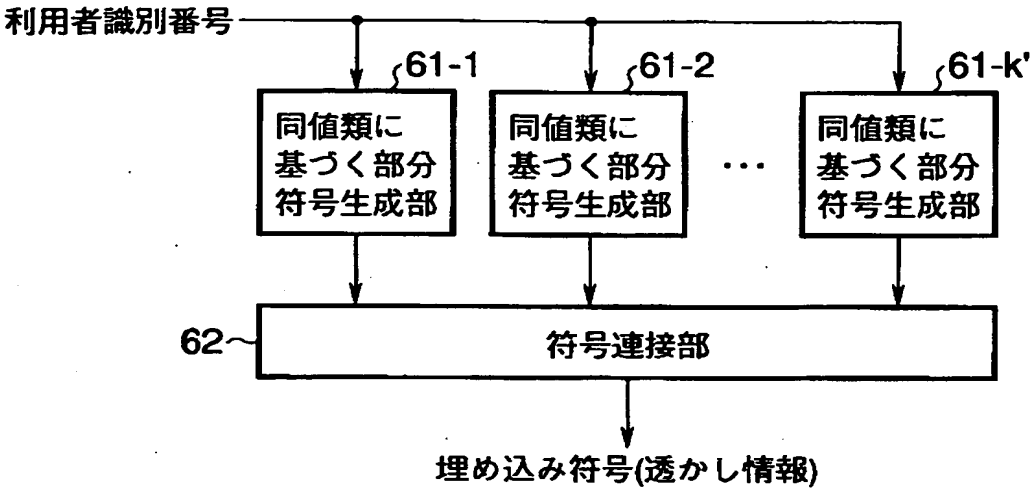
【図９】


スタート
i=0
i=k?
YES
NO
Rkの出力
エンド
i++
pi とri の入力
A≡(p1p2… pi-1)-1mod pi の計算
B≡(Ri-1-r1)mod pi の計算
C≡A×Bmod pi の計算
R ≡C×p1p2… pi-1 +ri の計算

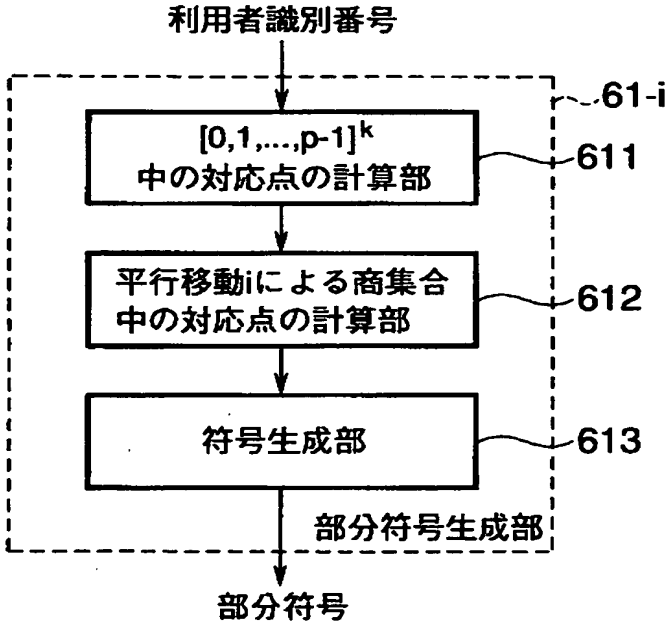
【図１０】


スタート
埋め込み済みコンテンツの入力
S11
埋め込み符号の検出
S12
S13
結託の有無の判定
YES
NO
S14
利用者識別番号の計算
S15
利用者識別番号の出力
結託者番号の計算
S17
結託者番号の出力
S16
結託存在
信号の出力
S18
エンド

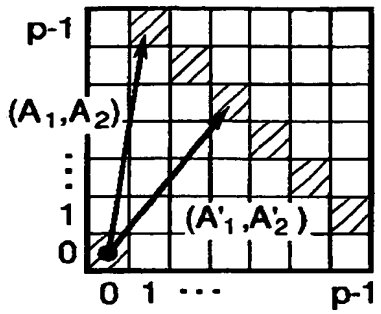
【図１１】


利用者識別番号
61-1
61-2
61-k'
同値類に基づく部分符号生成部
同値類に基づく部分符号生成部
・・・
同値類に基づく部分符号生成部
62
符号連接部
埋め込み符号(透かし情報)

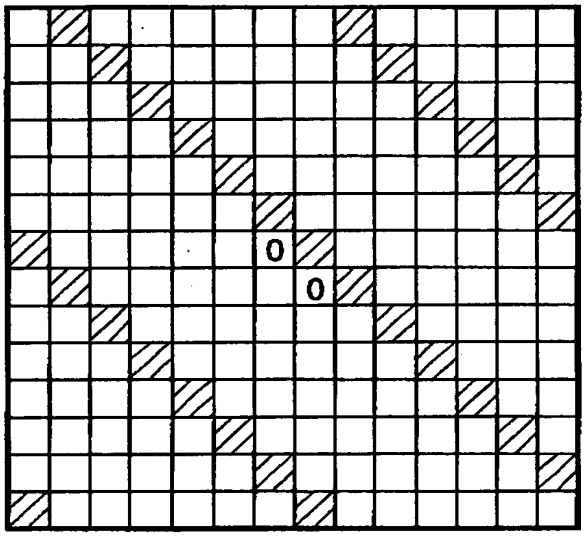
【図１２】


利用者識別番号
61-i
[0,1,...,p-1]^k 中の対応点の計算部
611
平行移動iによる商集合中の対応点の計算部
612
符号生成部
613
部分符号生成部
部分符号

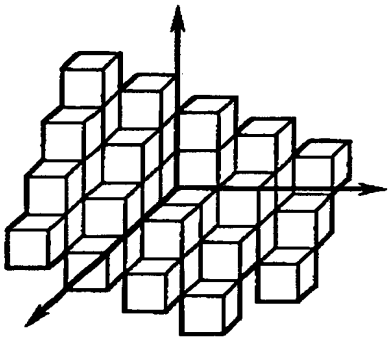
【図１３】



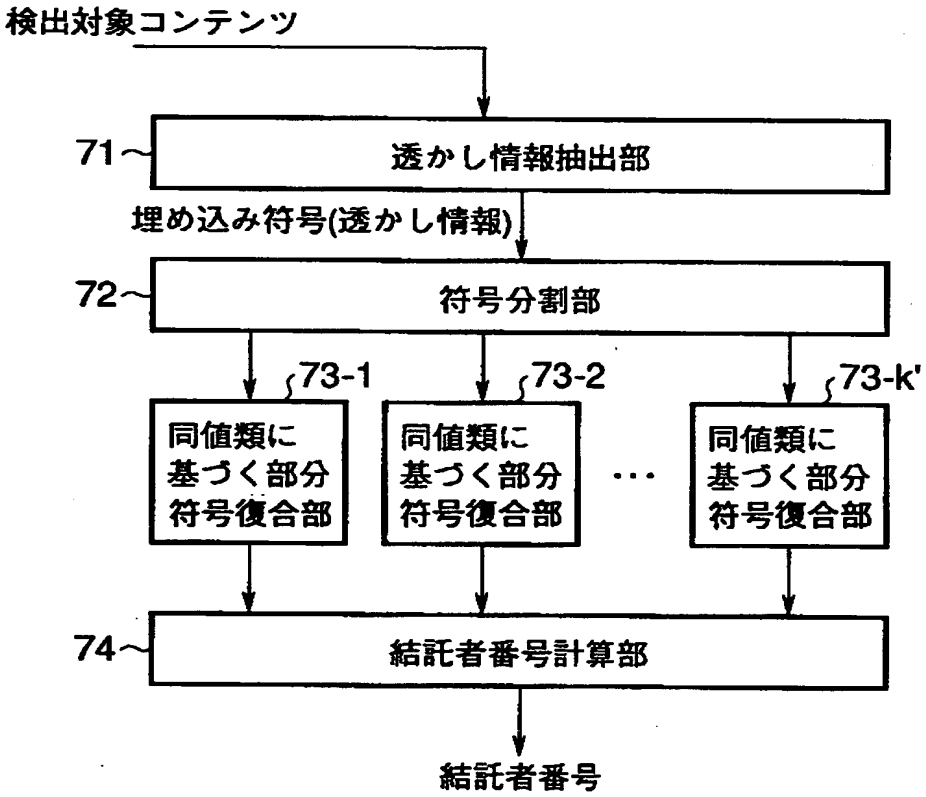
【図１４】



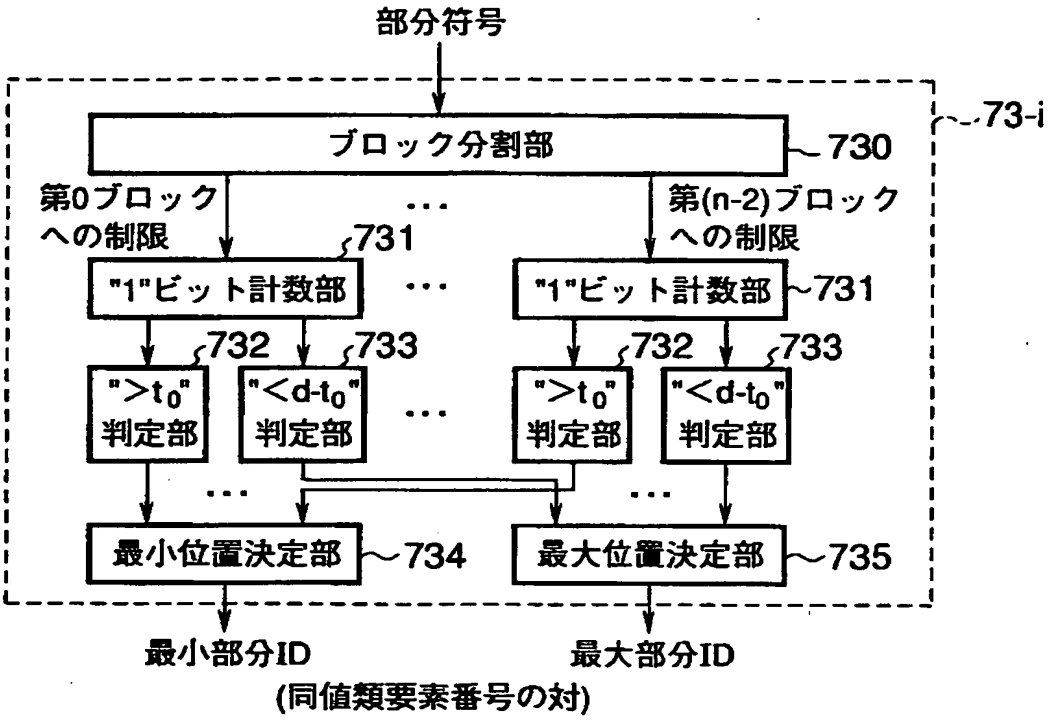
【図１５】



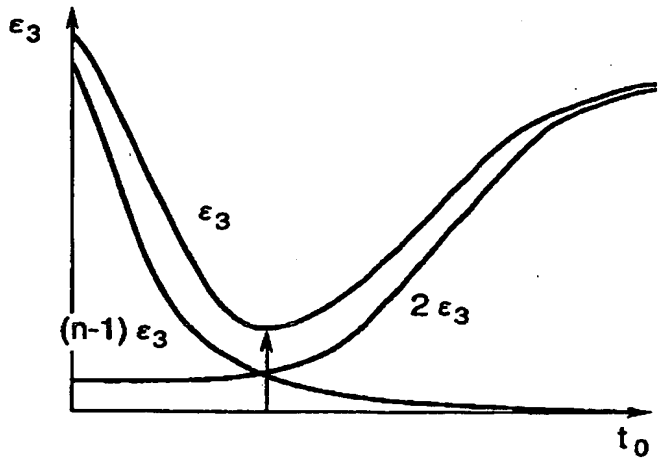
【図１６】


検出対象コンテンツ
71
透かし情報抽出部
埋め込み符号(透かし情報)
72
符号分割部
73-1
73-2
73-k'
同値類に基づく部分符号復合部
同値類に基づく部分符号復合部
・・・
同値類に基づく部分符号復合部
74
結託者番号計算部
結託者番号

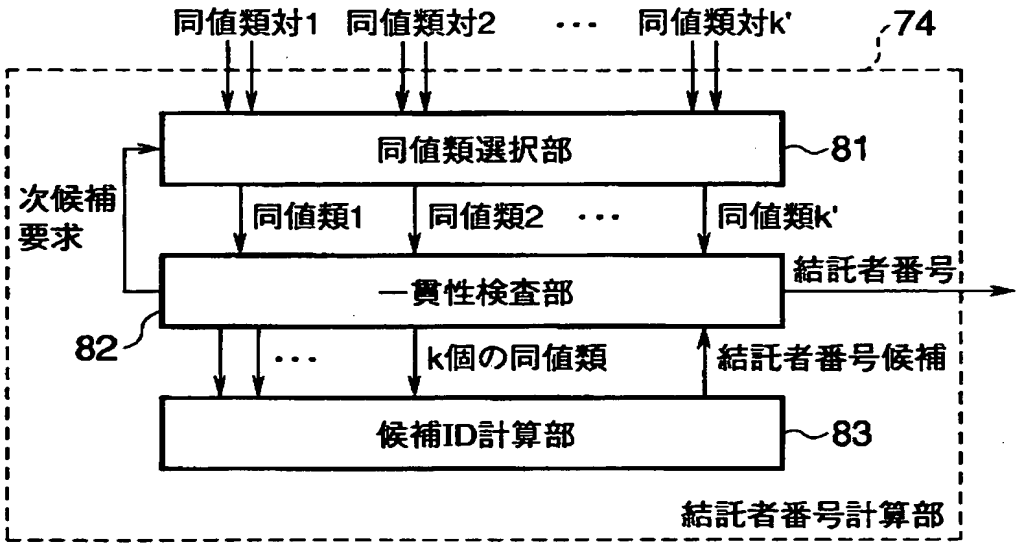
【図１７】


部分符号
73-i
ブロック分割部
730
第0ブロックへの制限
第(n-2)ブロックへの制限
731
"1"ビット計数部
732
733
">t0"判定部
"<d-t0"判定部
最小位置決定部
734
最大位置決定部
735
最小部分ID
最大部分ID
(同値類要素番号の対)

【図１８】


ε3
ε3
2ε3
(n-1)ε3
t0

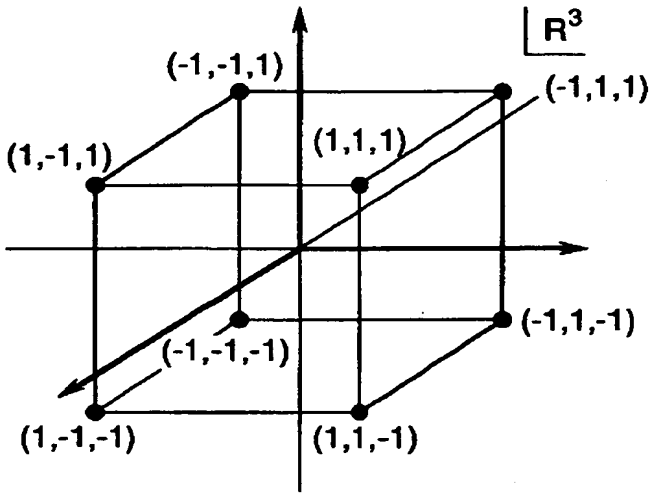
【図１９】



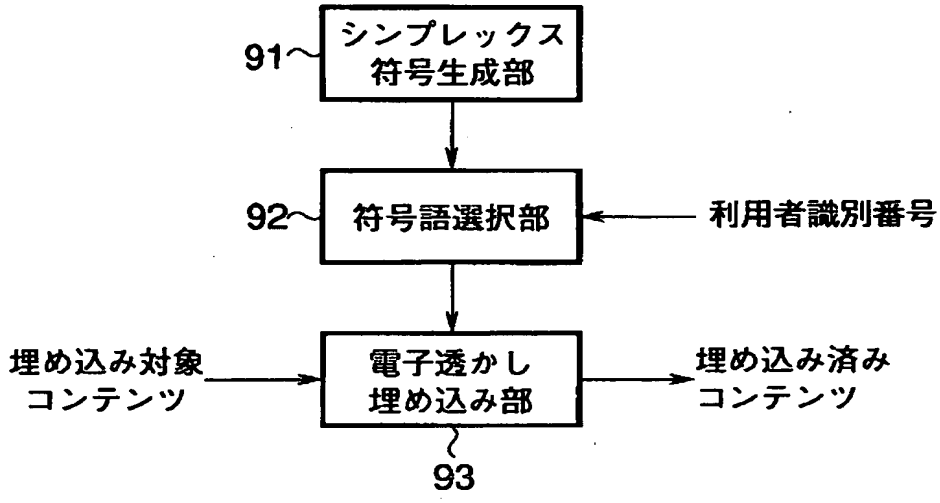
【図２０】

利用者識別番号	B(0)	B(1)	・・・	B(S_{min})	・・・	B(S_{max})	・・・	B(n-3)	B(n-2)
0	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1
1	0・・・0	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1
・・・									
S_{min}	0・・・0	0・・・0	0・・・0	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1	1・・・1
・・・									
S_{max}	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	1・・・1	1・・・1	1・・・1	1・・・1
・・・									
n-2	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	1・・・1
n-1	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0	0・・・0

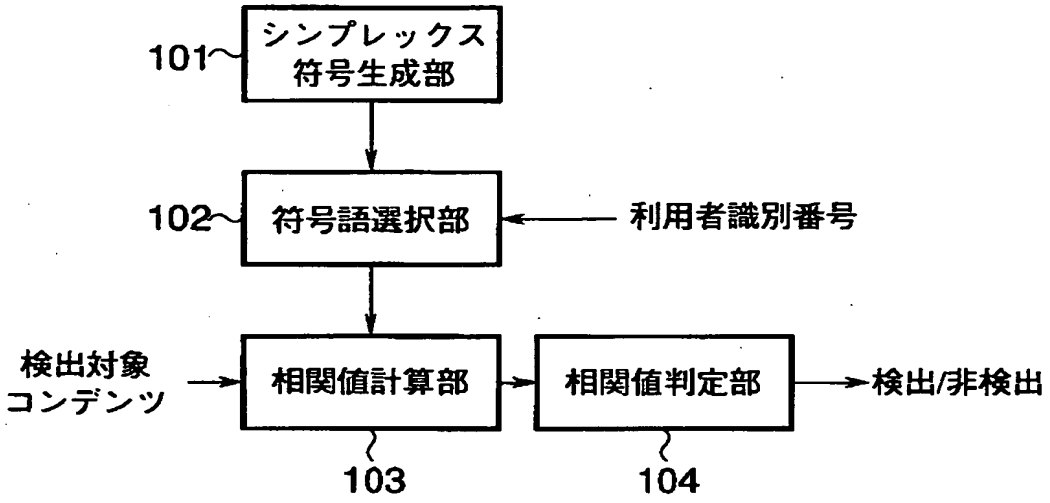
【図２１】


R3
(-1,-1,1)
(-1,1,1)
(1,-1,1)
(1,1,1)
(-1,1,-1)
(-1,-1,-1)
(1,-1,-1)
(1,1,-1)

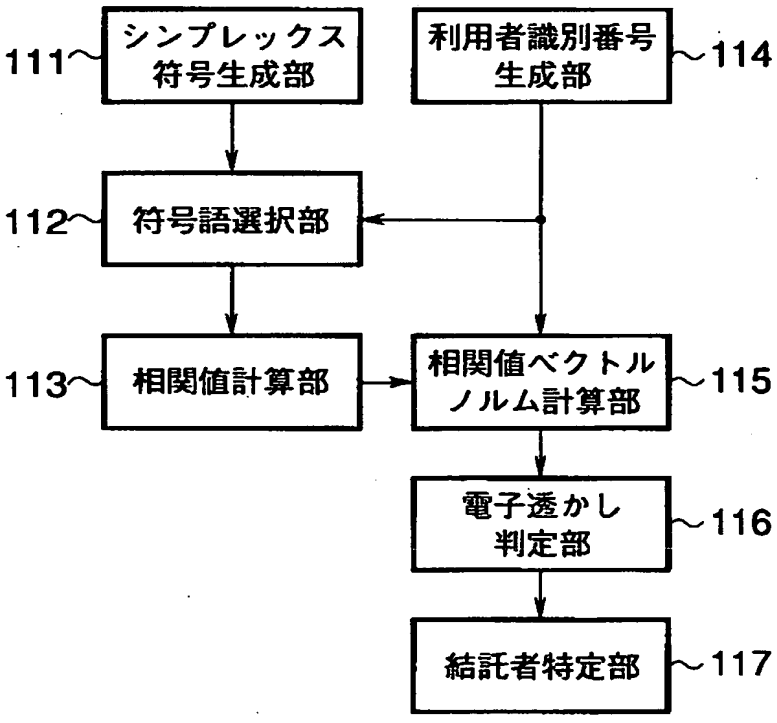
【図２２】


91
シンプレックス
符号生成部
92
符号語選択部
利用者識別番号
埋め込み対象
コンテンツ
電子透かし
埋め込み部
埋め込み済み
コンテンツ
93

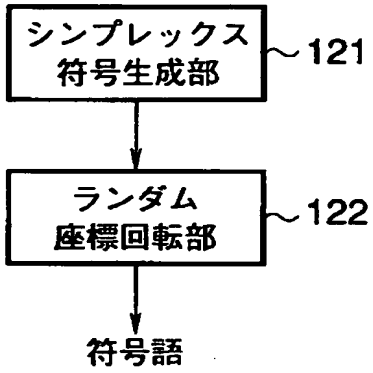
【図２３】


101
シンプレックス
符号生成部
102
符号語選択部
利用者識別番号
検出対象
コンデンツ
相関値計算部
相関値判定部
検出/非検出
103
104

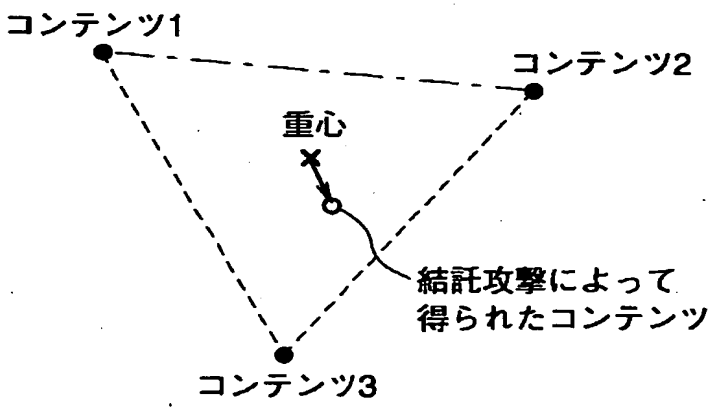
【図２４】


111
シンプレックス
符号生成部
利用者識別番号
生成部
114
112
符号語選択部
113
相関値計算部
相関値ベクトル
ノルム計算部
115
電子透かし
判定部
116
結託者特定部
117

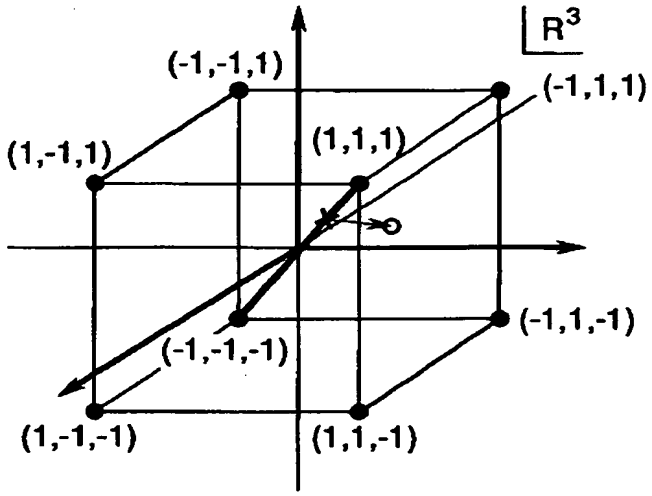
【図２５】


シンプレックス
符号生成部
121
ランダム
座標回転部
122
符号語

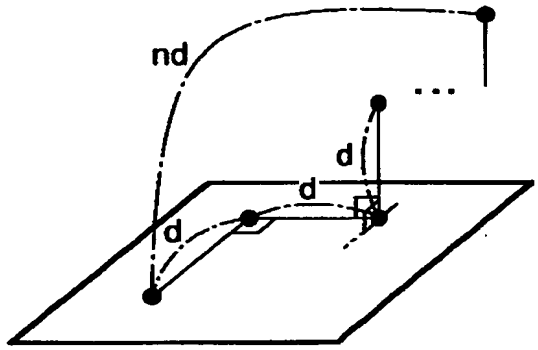
【図２６】


コンテンツ1
コンテンツ2
重心
結託攻撃によって
得られたコンテンツ
コンテンツ3

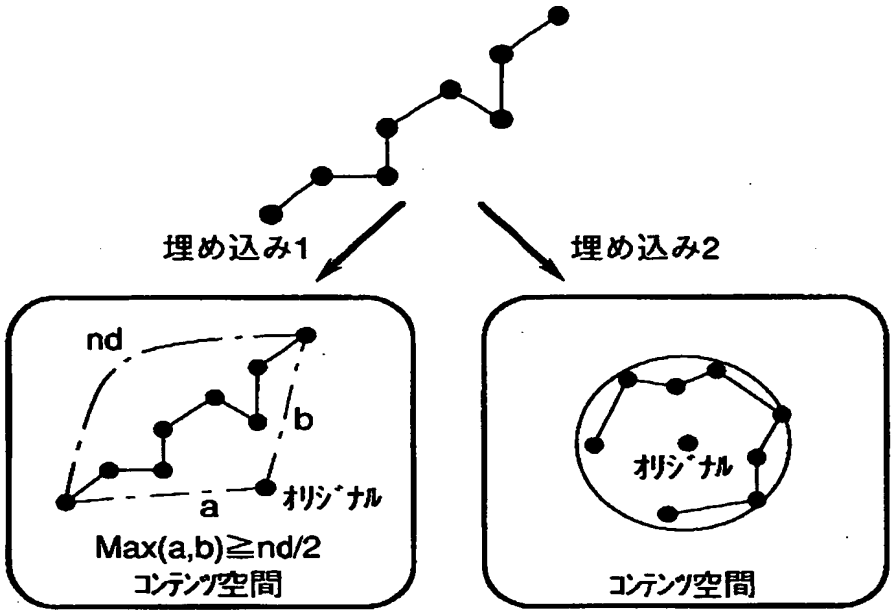
【図２７】



【図２８】



【図２９】



【書類名】　　要約書

【要約】

【課題】結託攻撃への耐性を持ち、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置を提供する。

【解決手段】剰余計算部２２－１，２２－２，…，２２－ｋ′により利用者識別番号に対して法記憶部２１－１，２１－２，…，２１－ｋ′に記憶された複数の素数を法とする剰余をそれぞれ求め、これらの剰余及び符号化パラメータ記憶部２３に記憶されたパラメータに基づいて、部分符号生成部２４－１，２４－２，…，２４－ｋ′により所定のビット数を一単位とする連続した１の列及び０の列で構成される部分符号をそれぞれ生成し、これらの各部分符号を連接部２５で連接して、透かし情報を構成する埋め込み符号を生成する。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝